TRICARE Management Activity

Protected Health Information Management Tool (PHIMT)

Training Reference: Privacy Specialist Manual
Version 1.0

Prepared By:
Booz Allen Hamilton

This page lists all of the changes that have been made to the PHIMT Privacy Specialist Manual throughout its development.

Version	Release Date	Summary of Changes

Table of Contents

1.0 INTRODUCTION TO PHIMT

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires a covered entity, (i.e., the Military Health System (MHS)) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than treatment, payment and healthcare operations (TPO). The MHS must be able to provide an accounting of those disclosures to an individual upon request. Authorizations and Restrictions from an individual to a covered entity are included in the information that is required for tracking purposes.

To comply with the requirements for disclosures, the TRICARE Management Activity (TMA) is providing an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures, authorizations, and restrictions that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures, if necessary.

The MTF should have knowledge of DoD 6025.18-R, Health Information Privacy Regulation. A MTF must provide an accounting of disclosures within 60 days of the request. If the covered entity cannot honor an accounting of disclosures within the 60-day period, it must provide information to the requestor as to the reason for the delay and expected completion date. The covered entity may extend the time to provide the accounting by no more than 30 days. Only one extension is permitted per request.

1.1 PHIMT REQUIREMENTS

Before using PHIMT it is necessary to understand and ensure the operating requirements are met. PHIMT has specific requirements for the operating system, browser, and plug-ins.

1.1.1 System Requirements

Using PHIMT requires a Microsoft Windows application: Windows XP (home, professional); Windows 2000 (standard, professional, advanced); or Windows 98.

<u>NOTE</u>: Windows NT does work with PHIMT in most cases, but some limitations may exist. Therefore, Windows NT is not supported for use with PHIMT.

1.1.2 Browser Requirements

PHIMT requires the use of Microsoft Internet Explorer, version 6.0 or above.

<u>NOTE</u>: Cookies and JavaScript should be enabled (these items are enabled in a default browser installation)

1.1.3 Plug-Ins

PHIMT requires the use of Adobe Acrobat, version 6.0 or above. The application will also work with version 5.0 but the latest version is recommended.

NOTE: To display the generated letters and reports in the browser, the Adobe Acrobat Plug-in is required. This is normally installed with Adobe Acrobat Reader. Download Adobe Acrobat for free at http://www.adobe.com.

2.0 GETTING STARTED

In PHIMT, the Privacy Specialist is usually the MTF's Privacy Officer. The Privacy Specialist approves and denies disclosure requests, and restricts and suspends disclosures. Much of this tasking is forwarded from the Regular User. In addition, the Privacy Specialist works closely with the User Admin in creating user roles within an organization and user-to-user relationships.

2.1 USER DEFINITIONS AND ROLES

Each User is assigned to one or more organizations (an organization is a logical or physical entity such as an MTF, a Service or TMA).

- Within an organization, each user can have one or more roles.
- A user can have the same roles in multiple organizations, or different roles in multiple organizations.
- Roles are inherited down the permission levels.

A **Role** is a named collection of permissions. Roles allow Users with the same permissions to be grouped under a unique name. PHIMT roles include: Regular User, User Admin, Privacy Specialist, and Tool Admin.

- A **Regular User** is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist.
- A **User Admin** is a local administrator for an MTF or a designated Service. This role allows one to add/modify users from within their Service and assigns roles. The email account administrators will handle this role for each MTF or Service.
- A **Privacy Specialist** is the Privacy Officer or MTF designee. This role allows the User to maintain disclosure reporting by approving and or denying various disclosure requests.
- A **Tool Administrator** has global access to the application and will be maintained by the HIPAA Support Center. This role allows the User to configure roles within MTFs, and create permissions within the application.

NOTE: Your particular user role will determine the PHIMT activities you are authorized to perform. For example, as a Privacy Specialist, you can perform only those activities listed on *the User, Admin, Patient, Requests, and Requester tabs. Different user roles are authorized to access different tabs.*

2.1.1 PHIMT Roles and Permissions

PHIMT roles and permissions are based on status-level relationships within service groups. These service groups consist of the Army, Navy, Air Force, and Coast Guard. Anyone in a given service group can be granted access to information required for them to perform their duties. Specific roles have corresponding permissions that determine who will have access to what. Individuals within PHIMT roles have access to information required for job performance as well as access to information accessible to those roles with fewer permissions. No individual will be granted access to information needed to perform duties that require a higher set of permissions. Those in roles with the highest levels of permissions will have access to all information within their service group. No individual within any service group will be granted access to information in a service group other than their own.

For example, the TMA (TRICARE Management Activity) and Support, Group A the top tier, occupies those roles with the highest levels of permissions. These individuals are granted access to all information within their Service Group. Those individuals in the Service Groups who occupy roles requiring a lower level of permissions, Group B the second tier, do not have access to the information accessible to those in the top tier. However, Group B does have access to the information in tier C, comprised of roles requiring even lower permission levels. The third tier, Group C, is comprised of offices and command centers within the service groups. This tier can only access information necessary for them to complete their responsibilities. They do not have access to information within the higher tiers. There is absolutely no viewing of another's information outside of your own service group.

2.1.2 Privacy Specialist Role

In PHIMT, the Privacy Specialist is usually a Privacy Officer within the facility or a designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amend requests, restrict and suspend disclosures, and issue complaints.

The Privacy Specialist understands how the MTF manages disclosures. Disclosure requests may be routed from a Regular User to the Privacy Specialist or from one Privacy Specialist to another. This process helps establish working relationships between the different PHIMT users.

2.1.3 Interaction with the User Admin

In order for PHIMT to be most beneficial, users within departments that manage Protected Health Information (PHI), are assigned roles with a varying degree of permissions. Some of the departments that the Privacy Officer may wish to grant access include, (but are not limited to):

- Medical records
- Release of information

- Patient advocate
- Patient's rights
- Privacy office

Some or all individuals within the various departments may be designated as Regular Users or Privacy Specialists.

The User Admin creates accounts and User-to-User Relationships as directed by you, in your role as the Privacy Officer. A collaborative effort is required to ensure the release of PHI is managed within PHIMT. Before establishing any accounts, you need to understand the way the MTF manages disclosures, the key individuals involved in the release of information and tracking of disclosures, and the approval process. The User Admin has a complementary knowledge base and understands how to create a workflow by routing the requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, if necessary. Multiple User-to-User Relationships can be established throughout the facility.

3.0 ACCESSING AND USING PHIMT

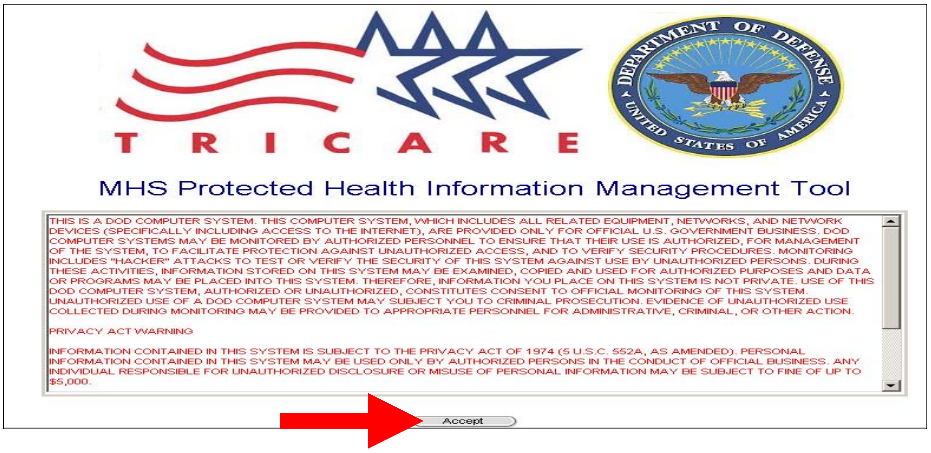
Now that you have an understanding of why PHIMT was developed and are familiar with its capabilities and system requirements, and have basic knowledge about your role as a Privacy Specialist, you are ready to access the application.

To login to the PHIMT application:

1. Enter the URL for PHIMT into the Web browser, https://phimt.tricare.osd.mil.

2. Read the Notice and Terms of Use.

3. Click on the Accept button.

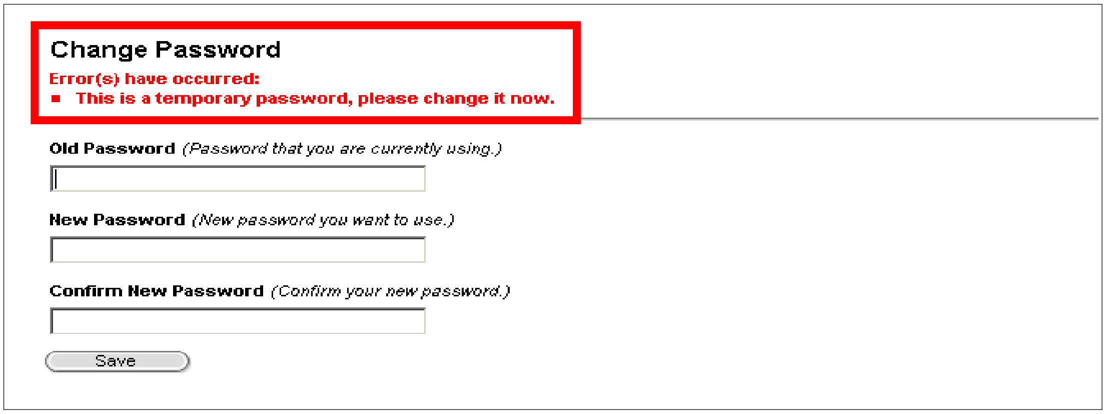


- Log in using the User Name and temporary Password that has been assigned to you by your User Admin.

4. Type in User Name and Password.

5. Click on the Login button.

- The first time you login you will be prompted to change your temporary password. Your new password must be 8 to 15 characters long and contain at least one of the following:
    - Alphabetic uppercase character
    - Alphabetical lower case character
    - Arabic numeral (0,1,2,3,4)
    - Non-alphanumeric special character (ex: !, @, #, etc.)



4.0 PRIVACY SPECIALIST TABS

In PHIMT, the Privacy Specialist has access to five tabs:

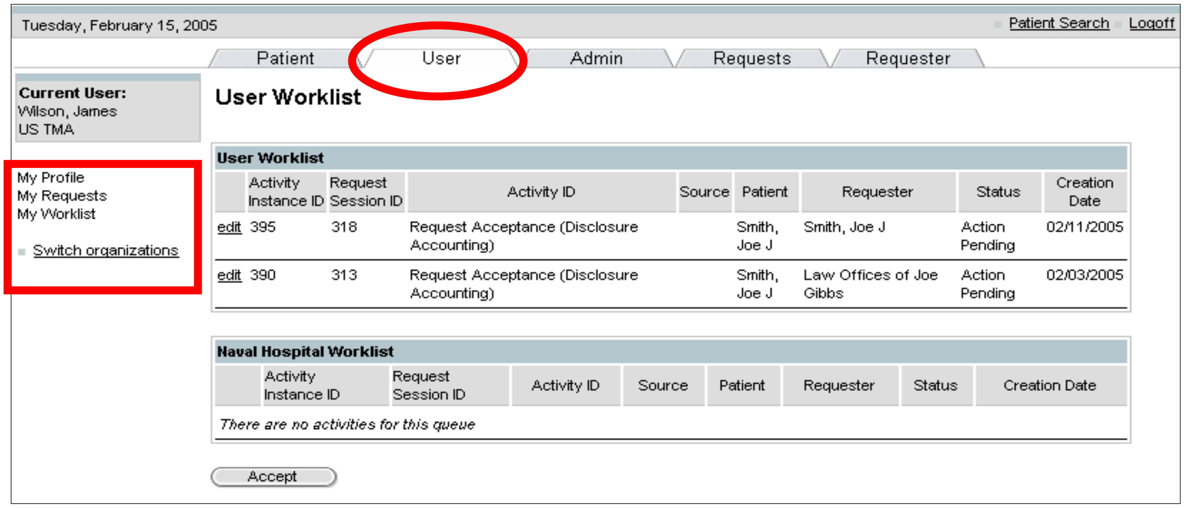
- User
- Patient
- Admin
- Requests
- Requester

4.1 USER TAB

The User tab contains all PHIMT User related information. The User tab is designed to track all tasks that are assigned to you. It allows you to perform desk duties including: updating your profile, viewing the status of your requests, and tracking your tasks.

As a PHIMT Privacy Specialist, you will have the authorization to perform certain activities in the User Tab by clicking on these hyperlinks:

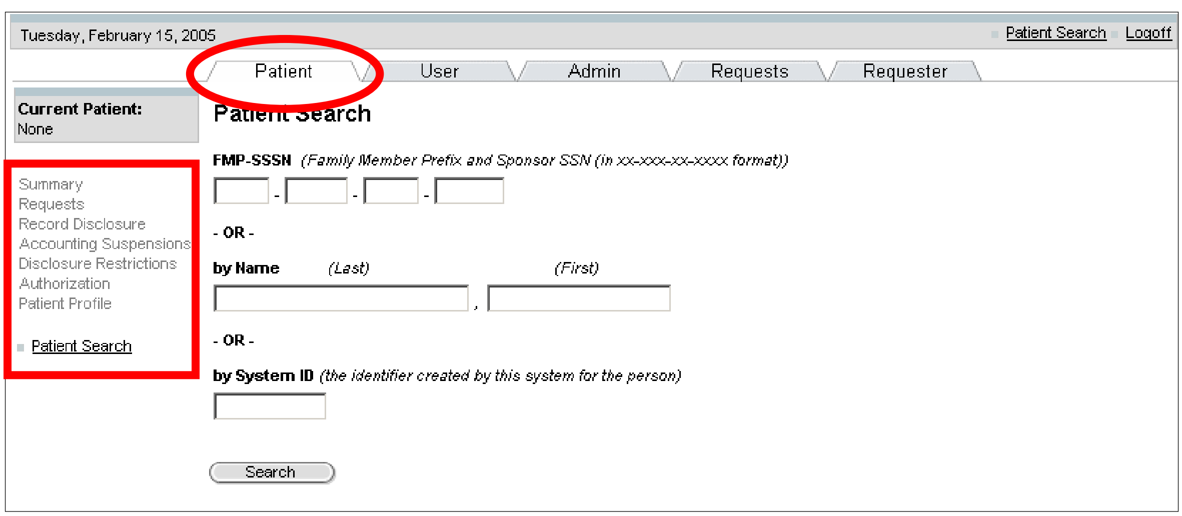
- My Profile - update personal information
- My Requests – view the status of all requests you initiated
- My Worklist – view and process all requests that have a task currently assigned to you
- Switch Organizations – switch your primary facility status to a different organization, if you are assigned to more than one organization.



4.2 PATIENT TAB

The Patient tab provides the Privacy Specialist with patient specific activities. These activities can be performed when accessed by the following hyperlinks:

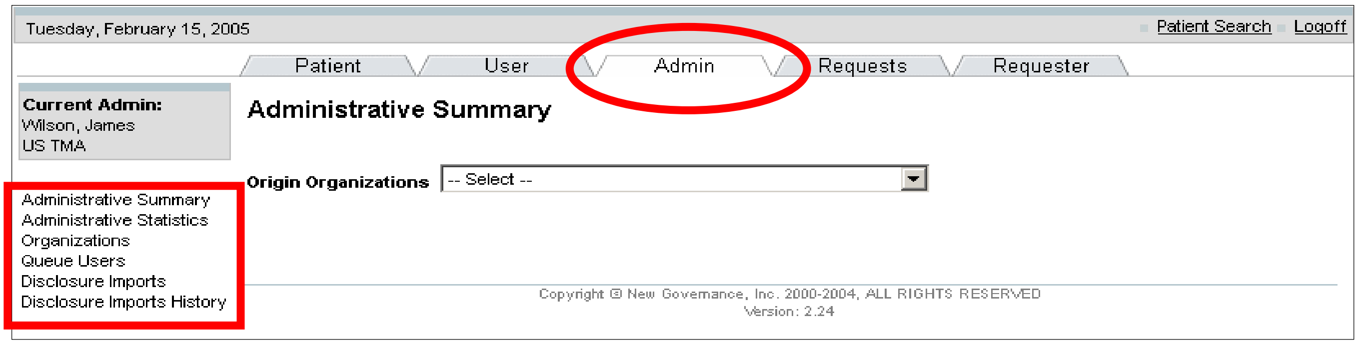
- Summary – view a synopsis of all disclosure activities for a particular patient
- Requests – perform the first step in initiating a disclosure activity
- Record Disclosure – record the release of protected health information
- Accounting Suspensions – temporarily postpone the release of protected health information
- Disclosure Restrictions – place constraints on the information being released or the recipient of that information
- Authorization – process an approval for a disclosure
- Patient Profile – create or edit patient information
- Patient Search – look for a particular patient in the PHIMT database



4.3 ADMIN TAB

The Admin tab allows the Privacy Specialist to access basic user admin activities that include maintaining organizations in the PHIMT database. This activity can be performed when accessed by the Organization Management hyperlink. The hyperlink allows you to maintain organizations by editing requested and recipient organizations.

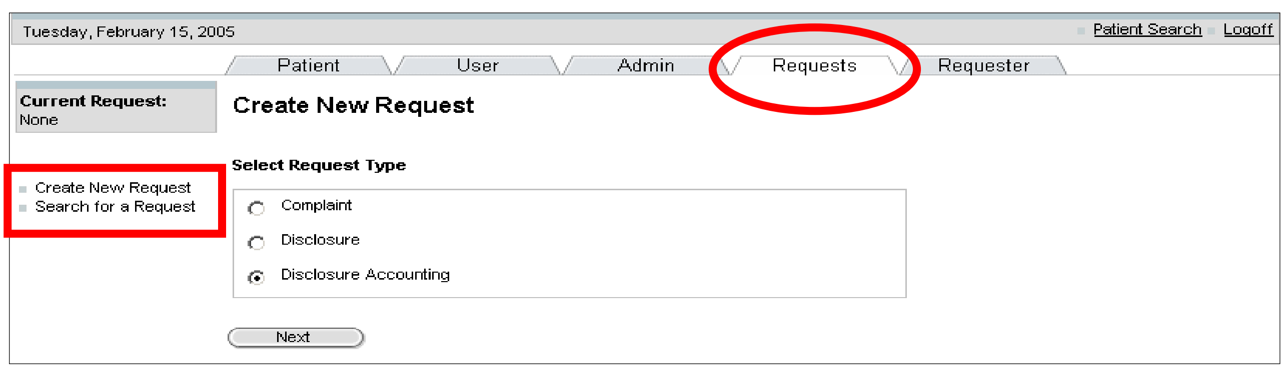
NOTE: If there is a request for a new type of administrative function, please contact your User Admin or the HIPAA Support Center.



4.4 REQUESTS TAB

The Requests tab allows the Privacy Specialist to access information about the activities requested by an individual or an organization. These activities can be performed when accessed by the following hyperlinks:

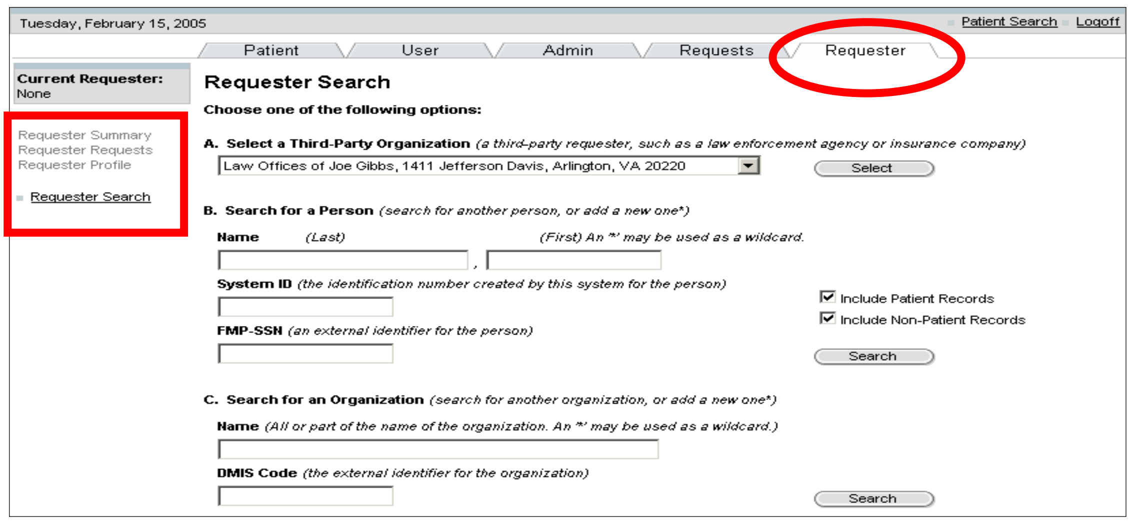
- Create New Request – initiate a request for a new disclosure activity
- Search for Request – look for a particular request
- Complaint – file a HIPAA grievance on behalf of a patient, against a person or an organization, and track as needed
- Disclosure – process a release of protected health information
- Disclosure Accounting – process a justification for a disclosure



4.5 REQUESTER TAB

The Requester tab allows the Regular User to access information about the individual or agency making a request for the disclosure. These activities can be performed when accessed by the following hyperlinks:

- Requester Summary – view a synopsis of all requests you initiated or those initiated by an individual or organization
- Requester Requests – view a listing of all requests you made or those made by an individual or organization
- Requester Profile – view information about the individual or organization making the request
- Requester Search **–** search for individual or organization making a request.



5.0 UNDERSTANDING PHIMT SCREENS

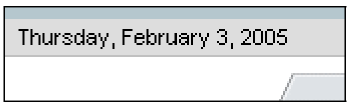
Each tab of the PHIMT screens contains some basic information that will be helpful to you when performing the various activities.

5.1 SCREEN FEATURES

There are many features to the PHIMT screen that you can use to navigate your way through the many disclosure activities you will perform. These features are discussed here.

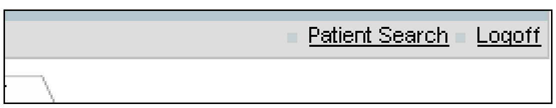
5.1.1 Date

The date displays the current weekday, month, day, and year in the upper left corner of the PHIMT screen.



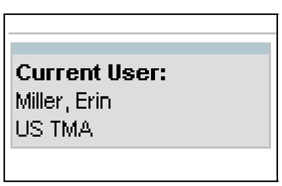
5.1.2 Navigational Options

Navigational options, such as patient search and logoff, provide directional hyperlinks that will help you to proceed through the PHIMT application. They are located in the upper right hand corner of the PHIMT screen.



5.1.3 Status Box

The gray status box shows current information and is located in the upper left hand corner of all PHIMT screens. The box displays the current user, user information such as organization and assigned role, patient information, and information about what disclosure activity is currently being performed. This information is updated when making inputs for various activities.



5.1.4 Activity Hyperlinks

The activity hyperlinks are located under the status box, on the left hand side of the PHIMT screen. This listing consists of hyperlinks for activities that can be performed while in a specific "tab." The hyperlinks may include: my worklist, patient profile, or authorization; depending on which tab you are using. Your user role will determine specific hyperlinks listed.

5.1.5 PHIMT Screen Tabs

PHIMT screen tabs are labels that are located at the top of the display screen. The tabs serve as file folders for different groupings of activities. The specific tabs will vary depending on what role you are assigned. Privacy Specialist tabs includes: User, Patient, Admin, Requests, and Requester. Each tab allows for different activities.

5.1.6 Screen Title

The screen title is located directly under the tabs and above the display screen. This is the title of the particular screen being displayed (ex. user worklist, patient search results).

5.1.7 Display Screen/Application Window

The display screen/application window is the PHIMT users work area. These screens contain various fields in which to provide required information for proceeding through the PHIMT activities. To assist with data input, PHIMT provides text boxes, windows, calendar icons, and drop down menus. All features may not be on a particular user screen:

- *Radio buttons* – Radio buttons appear as black dots to indicate selection. You can toggle the buttons between selected and not selected.

- *Check marks* – Check marks are used to indicate a done or un-done status. You can toggle the marks between checked and unchecked.
- *Drop down menus* – Drop down menus provide the user with a list of possible selections from which to choose. Clicking on a particular selection causes it to be selected and appear in the "window." You can change a selection by clicking the arrow on the menu box and then clicking on a different item.
- *Text boxes* – Text boxes are empty fields in which you can provide information. At times, this data is requested as additional comments or for supplemental information.
- *Calendar icons* – Calendar icons are provided to make it easier for you to input required dates. Date inputs are specific dates chosen by you to clarify time limits on various PHIMT activities. Choose a date by selecting the arrow in the date window. A calendar icon appears for easy inputs. Click on the desired date or use the arrows near the month and year headings to display a date not currently shown. The date you select will appear in the date window.
- *Action buttons* – Action buttons are used to guide you through the PHIMT steps and processes. Click on these buttons to proceed through various activities. Examples of these buttons include: Next, Save, Create, and Update.

<u>NOTE</u>: These features will be discussed when they are used in an activity.

5.2 PHIMT ERROR MESSAGES

PHIMT issues error messages when an entry or selection is not appropriate or complete. The message begins "Error(s) have occurred" and then follows with a bulleted list of the errors. For example, if you try to route an activity to someone who does not have access to that information, or you are not authorized to route the information to that particular person, PHIMT will display a message that indicating that you do not have the authority to perform that task. If you have not provided information for all the required data fields, PHIMT will issue a message indicating that information is missing. Once the error has been corrected, you can proceed to the next step in the PHIMT activity.

6.0 USER TAB ACTIVITIES

The hyperlinks on the User tab allow you to perform "desk duties" such as updating your user profile information, viewing requests you have made, and viewing your tasks, and switching your organization. A discussion on using the User tab hyperlinks follows.

6.1 MY PROFILE

The My Profile hyperlink brings you to the User Profile screen (shown below). This screen allows you to update or change your personal information such as: password, phone number, email address, signature block (used for personal or professional titles and credentials) and provide additional comments. Note the area for user roles, located on the bottom of the screen is not active. Only the User Admin has authorization to perform that activity. You also cannot change your User or system ID, user-to-user relationships, or user roles. The User Admin manages those. However, you can change backup person relationships (discussed later in the guide).

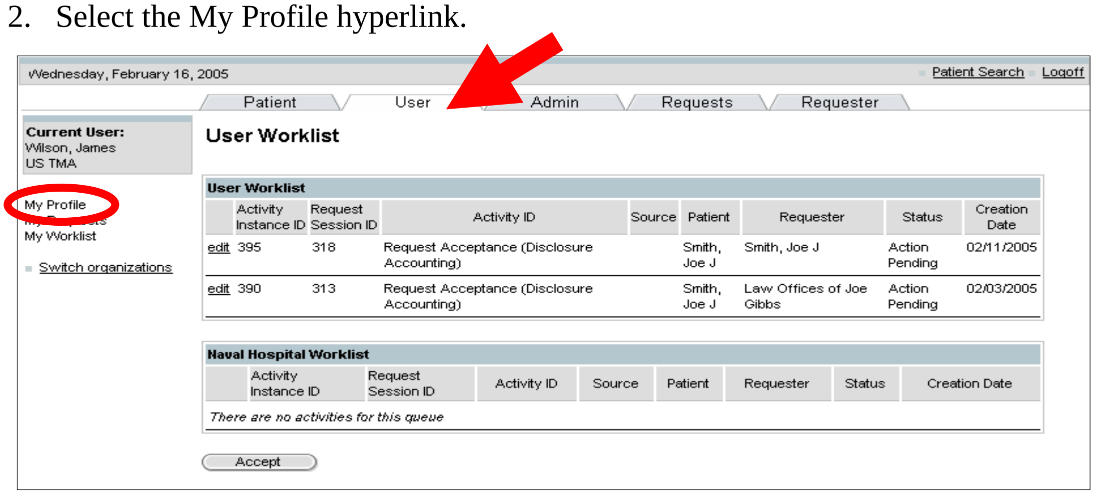
<u>NOTE</u>: When entering a phone number, remember that it will display on all correspondence when generated.

<u>NOTE:</u> PHIMT contains profiles for all users within the system. It is important to keep your personal information up to date. Therefore, you should update all personal information as it changes.

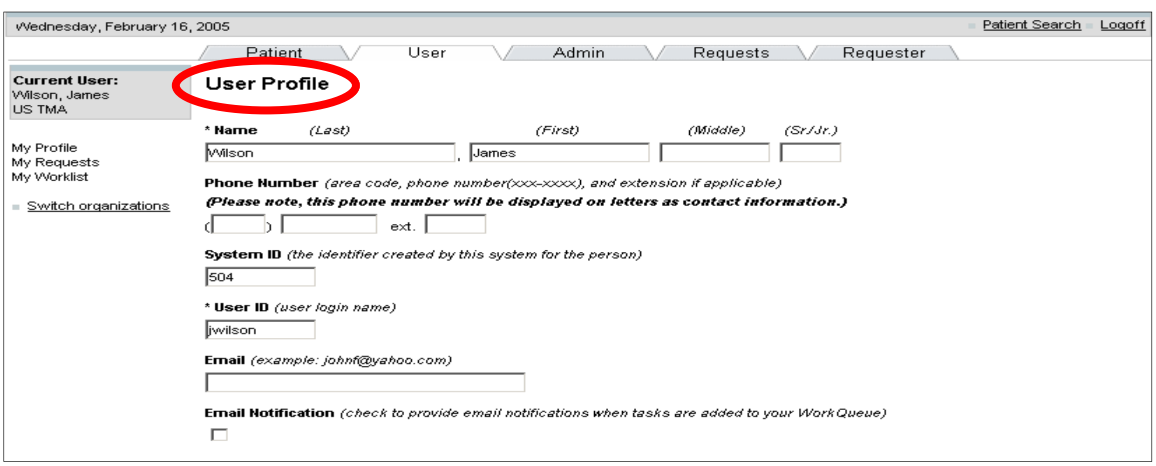
To update your user profile:

1. Select the User Tab.

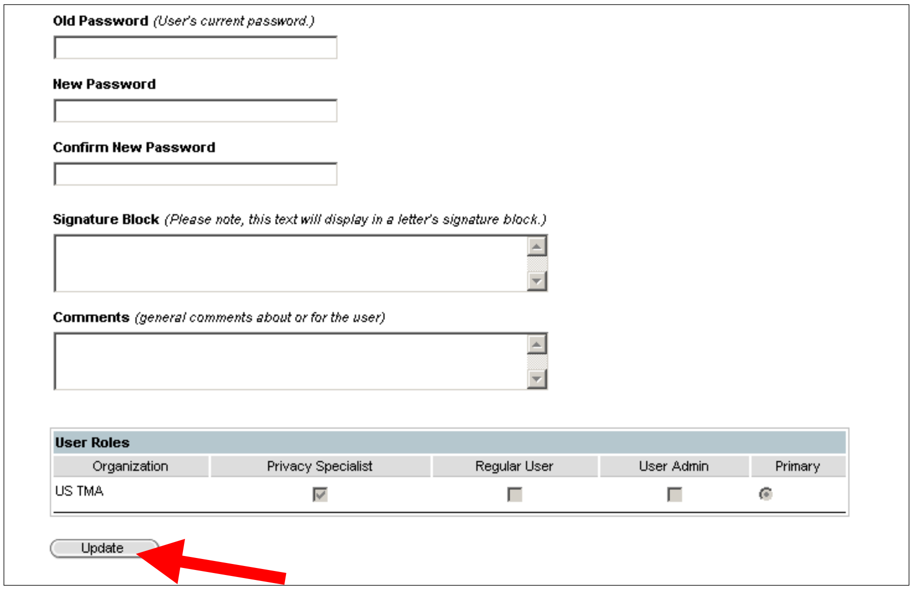
2. Select the My Profile hyperlink.



3. Enter your updated information in the information fields. (Changes can be made to any of the fields in the User Profile screen, except the System ID).



4. Click on the Update button.



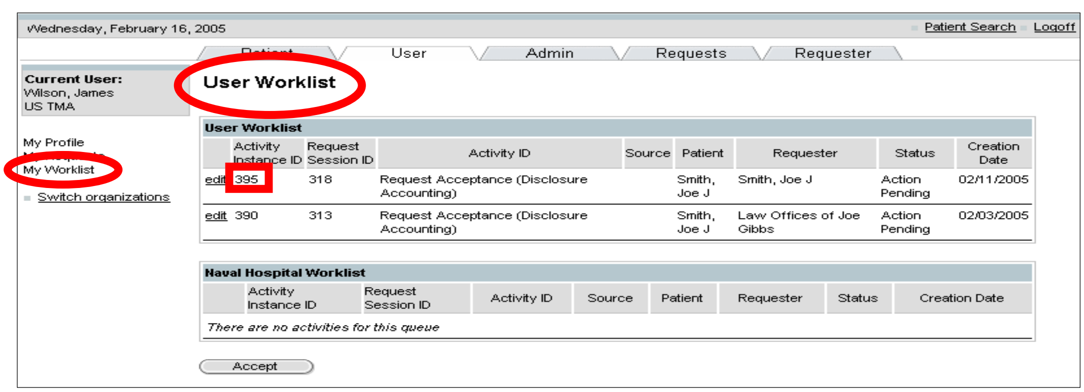
- Your new information will appear in the appropriate fields.

6.2 MY REQUESTS

The My Requests hyperlink brings you to the User Requests screen that allows you to view all PHIMT activity requests that you have made. To view a detailed summary of a specific request, select the Request Session ID.

6.3 MY WORKLIST

The My Worklist hyperlink brings you to the User Worklist screen (shown below) and allows you to view and process all requests that have a task currently assigned to you. My Worklist serves as your electronic inbox. You should review your User Worklist to verify any tasks that have been assigned to you. To view more information on a particular activity, select the Instance ID for that activity.



6.4 SWITCH ORGANIZATIONS

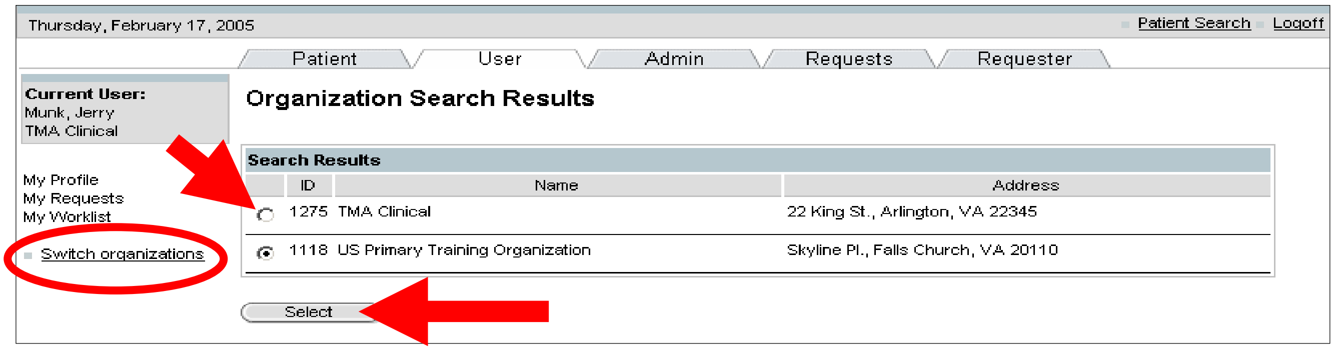
Switch Organizations brings you to the Organization Search Results screen (shown below) and allows you to switch the status of your primary facility to a different facility, if you are assigned to more than one organization. For example, if you wanted to change your primary organization from US Primary Training Organization to TMA Clinical; just select the radio button next to the desired selection, and choose Select. Your primary status change will be displayed in the status box.

To switch your organization:

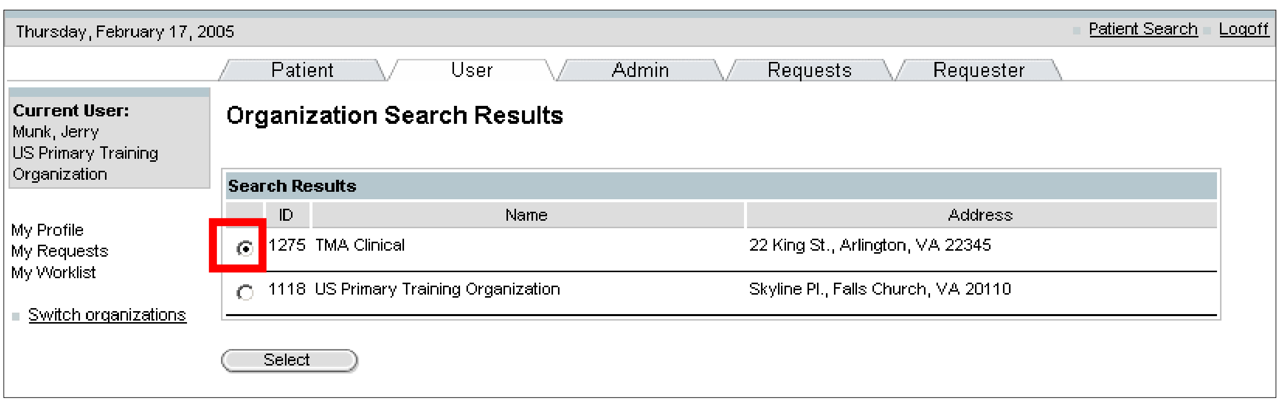
1. Select the Switch Organizations hyperlink on the User Tab.

2. Select the organization you want using the radio button.

3. Click on the Select button.



- The Organization Search Results screen now shows the radio button located near the facility you selected. The new selection is also reflected in the status box.



7.0 PATIENT TAB ACTIVITIES

The Patient tab allows you to view summaries, make requests, record disclosures; and create accounting suspensions, disclosure restrictions, authorizations, and patient profiles. It also allows you to search for patients. Two of the most common activities performed on the Patient tab are Patient Search and Create Patient. We will focus on these two activities here. The more complex Privacy Specialist activities using the Patient tab will be discussed in the Privacy Specialist Activities section.

7.1 PATIENT SEARCH

PHIMT allows you to use its search feature to find a patient that has already been added to the system.

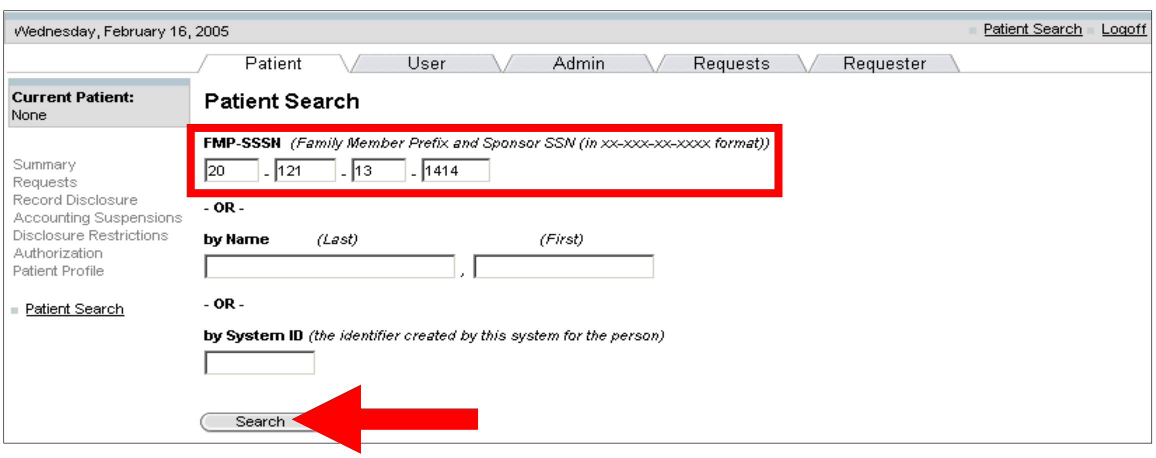
To search for a patient:

1. Select the Patient Tab.

2. Enter the search criteria. (You can search for a patient by the Family Member Prefix (FMP) Sponsor's SSN or by the patient's name).

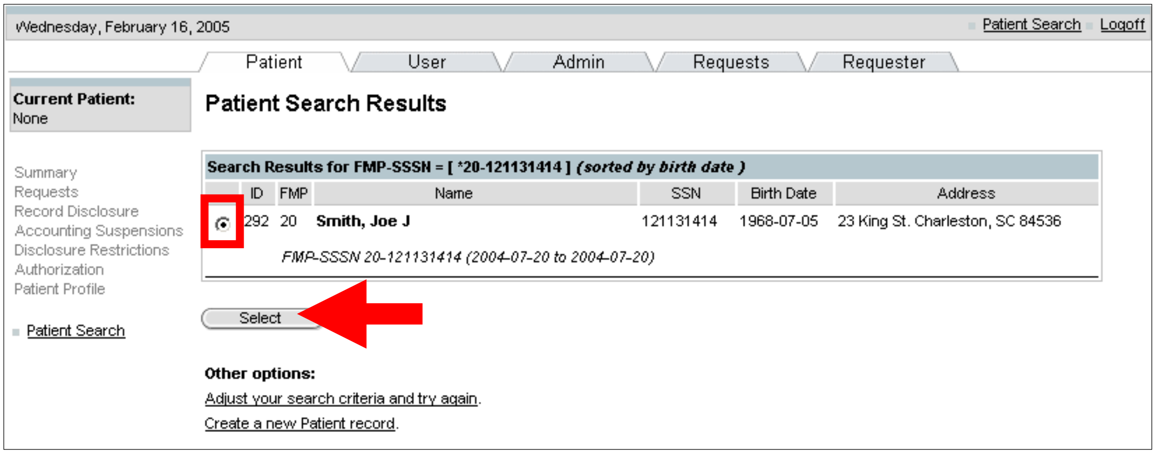
   (*NOTE: If you do not know how to spell the last name, just enter the first few letters and an asterisk. PHIMT will find the correct spelling*).

3. Click on the Search button.

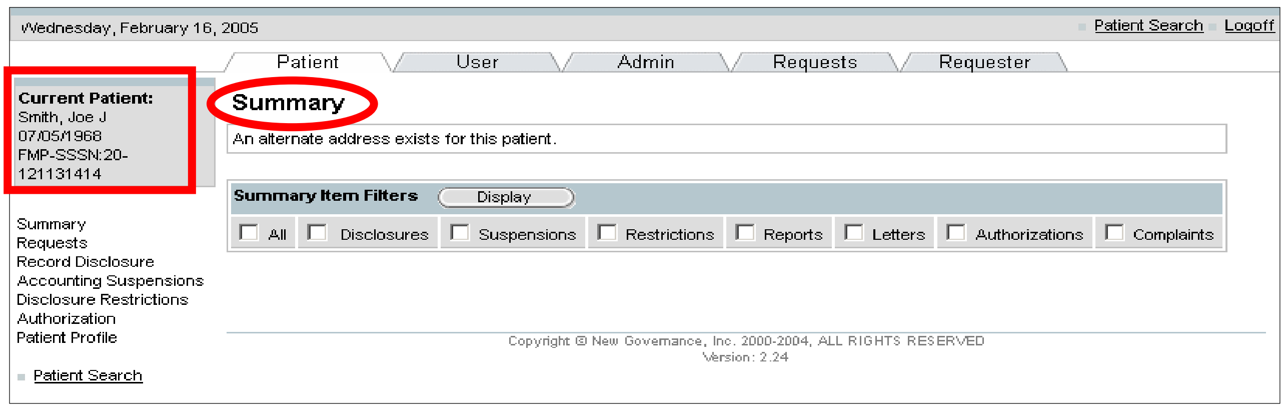


4. Select the patient from the Patient Search Results screen.

5. Click on the Select button.



- The Patient Summary Screen appears and the current patient is displayed in the status box.



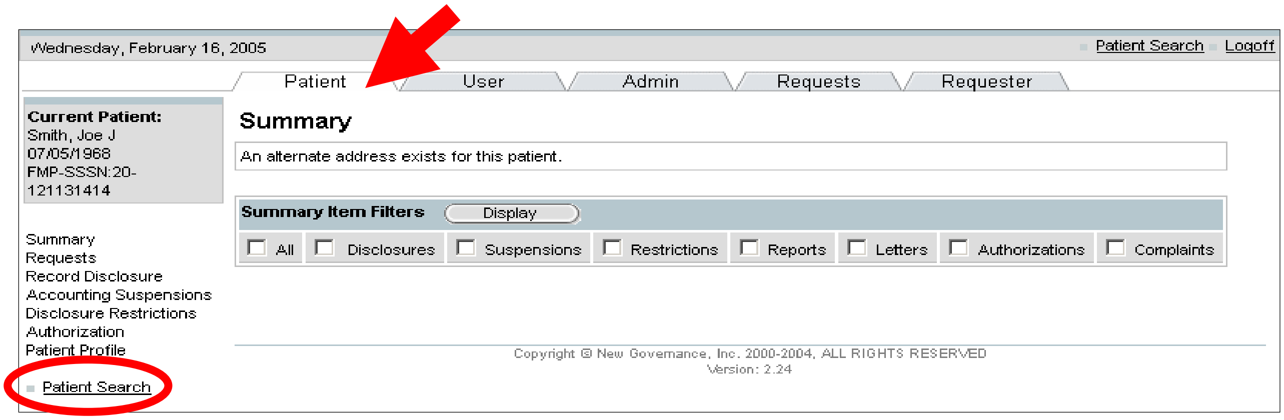
7.2 CREATE PATIENTS

When adding a new patient record, conduct a search within the system initially to ensure that the patient does not already exist. Patient records must be added to the system before disclosures, authorizations or restrictions can be documented.

To create a patient:

1. Select the Patient Tab.

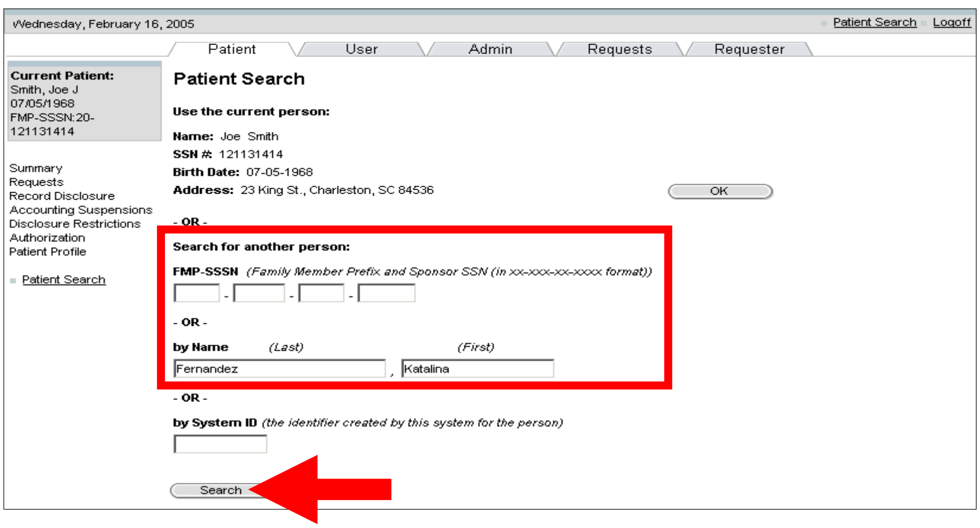
2. Select the Patient Search hyperlink.



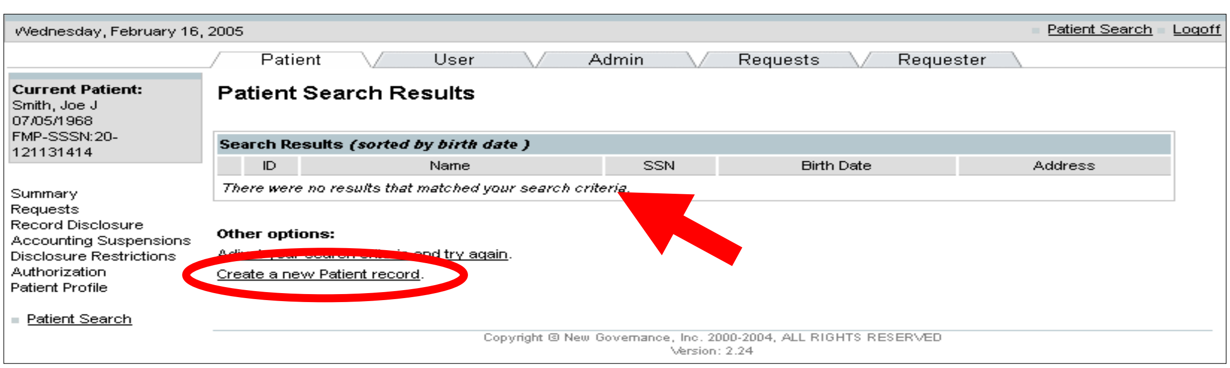
3. Enter the patient search criteria. (You can search for a patient by the Family Member Prefix (FMP) Sponsor's SSN or by the patient's name).

   <u>NOTE</u>: If you do not know how to spell the last name, just enter the first few letters and an asterisk. PHIMT will find the correct spelling.

4. Click on the Search button.

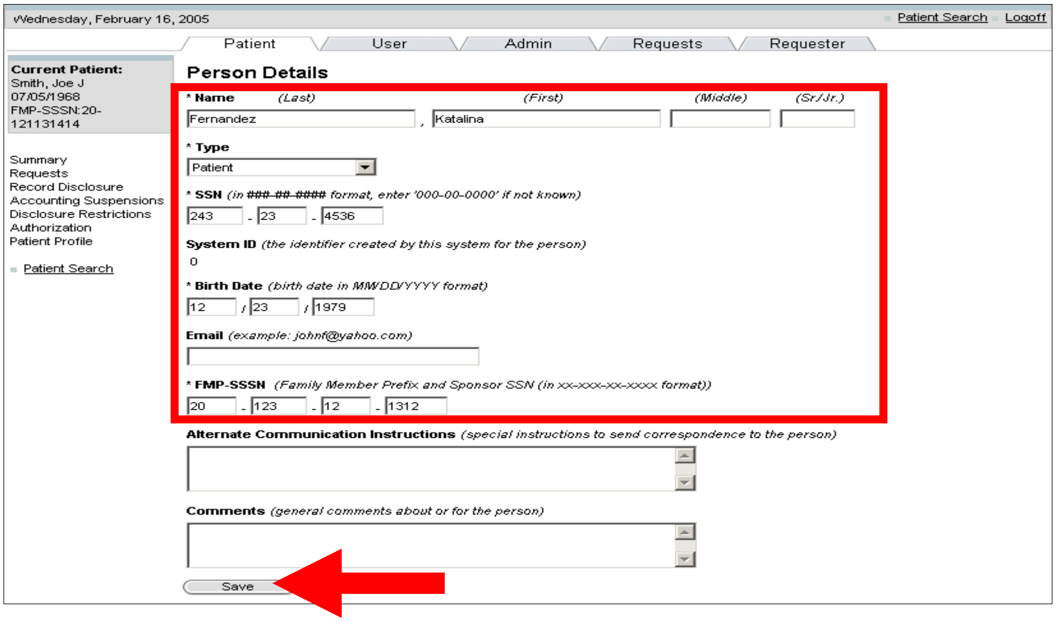


5. If no results matched your search, select the Create a New Patient Record hyperlink.



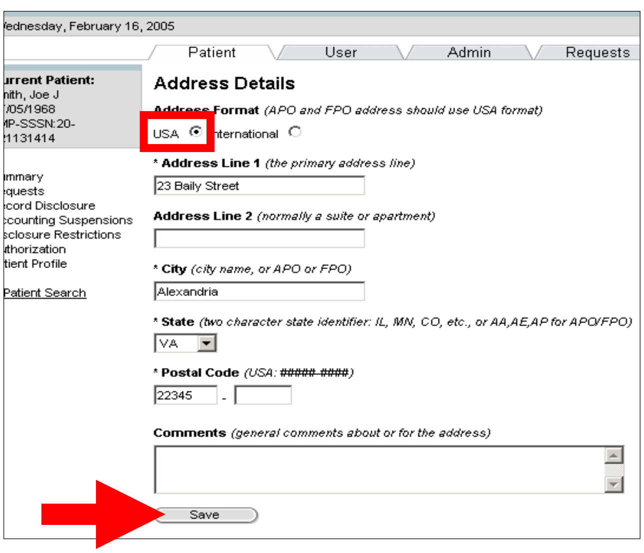
6. Enter the patient's information: (name, type, SSN, birth date, email, FMP-SSSN).

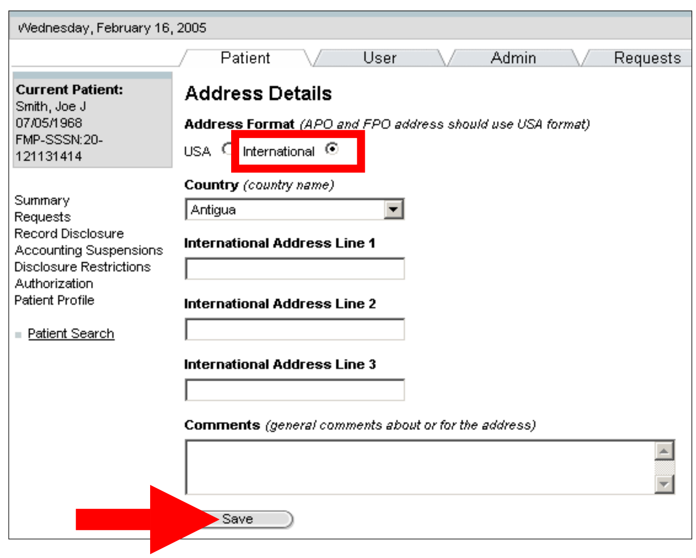
7. Click on the Save button.



8. Enter the Address Details (USA or International format).

9. Click on the Save button.





- The patient summary screen for the new patient will appear. (The patient is brand new so no specific patient information will be displayed at this time.) The information is also displayed in the status box.

8.0 PRIVACY SPECIALIST ACTIVITIES

As a Privacy Specialist you are authorized to perform specific activities including: approving disclosures, approving accounting of disclosures, recording complaints, recording disclosure restrictions, generating authorizations, revoking authorizations, and performing accounting suspensions. Instructions for performing these activities are provided in this section.

8.1 RECORD DISCLOSURES

The Privacy Specialist can use either the Disclosure Request or the Disclosure hyperlink to record disclosures. The Disclosure Request allows for forwarding the disclosure for approval or denial. The Disclosure hyperlink allows for immediate approval or denial.

If you're using the Disclosure Request you can enter Action Requested from the Action drop down menu, route it to your own worklist for later approval/denial, or route it to another Privacy Specialist.

If you're using the disclosure hyperlink you can complete the Disclosure in the Disclosure Status Field. Select Save when you have completed all fields pertaining to the disclosure.

NOTE: The Disclosure Type and Disclosure Purpose cannot be set to Undefined.

To record a disclosure:

1. Select the Patient Tab.

2. Enter the patient search criteria. (You can search for a patient by the Family Member Prefix (FMP) Sponsor's SSN or by the patient's name).

3. Click on the Search button.

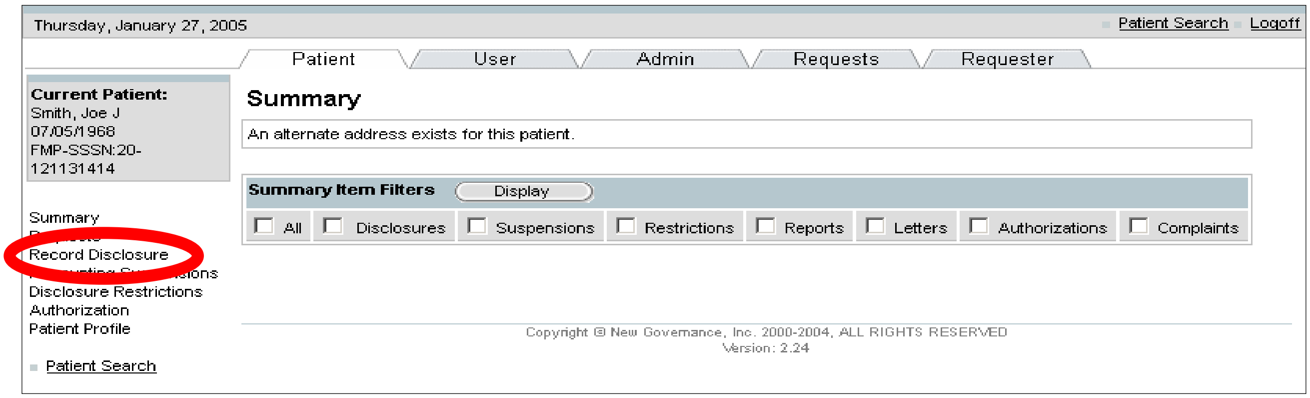
4. Select the patient from the Patient Search Results screen.

5. Click on the Select button.

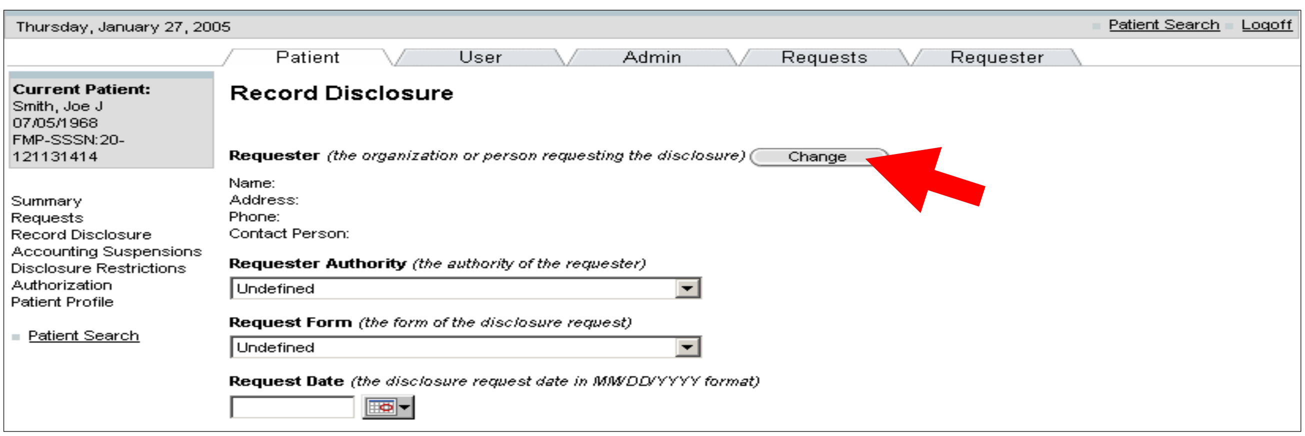
The Patient Summary screen appears.

NOTE: The steps 1-5 for recording a disclosure are the same as steps 1-5 in section 7.1 Patient Search. Refer to section 7.1 Patient Search for screen displays of steps 1-5.

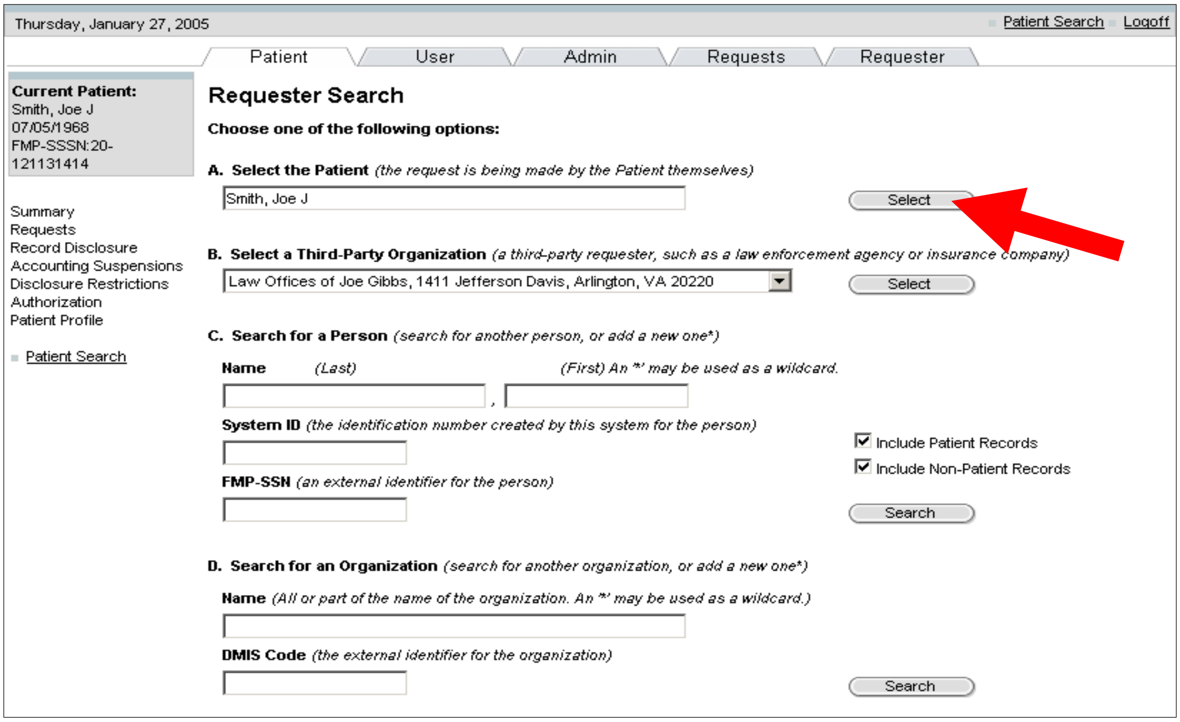
6. Select the Record Disclosure hyperlink on the Patient Summary screen.



7. Click on the Change button to change or update the requester.

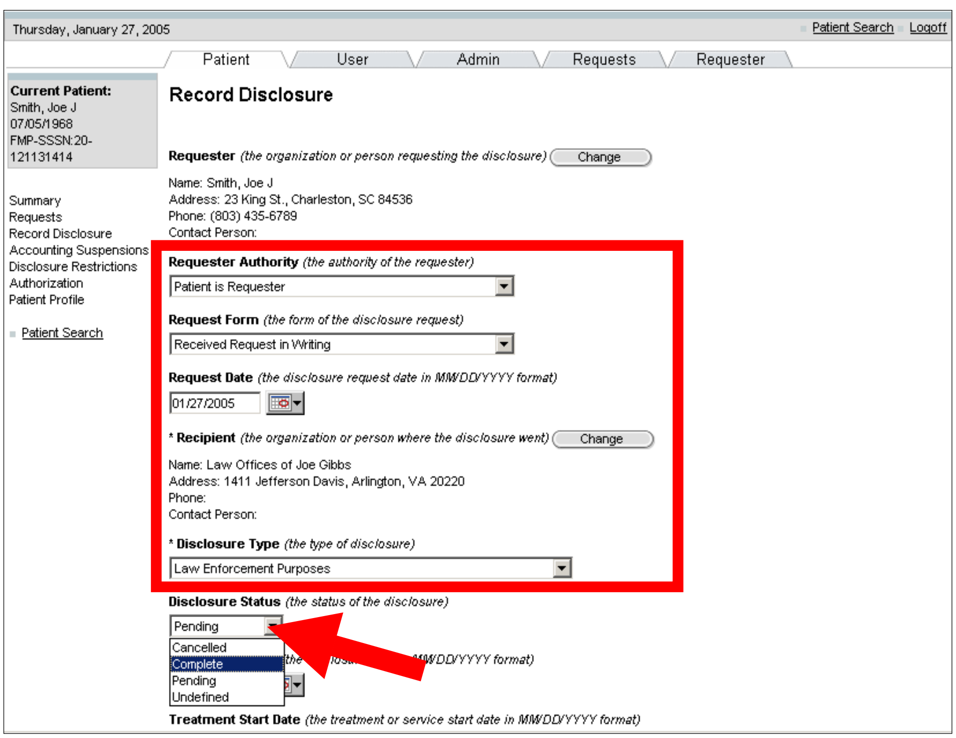


8. Select the requester.

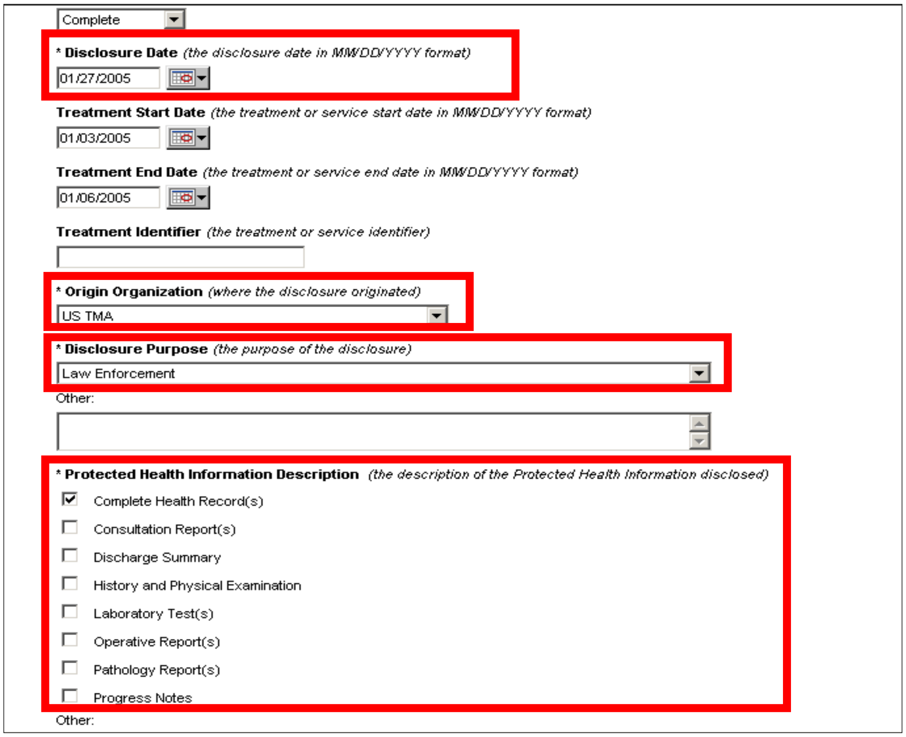


9. Record the Disclosure details: requester authority, form, date, recipient, and disclosure type.

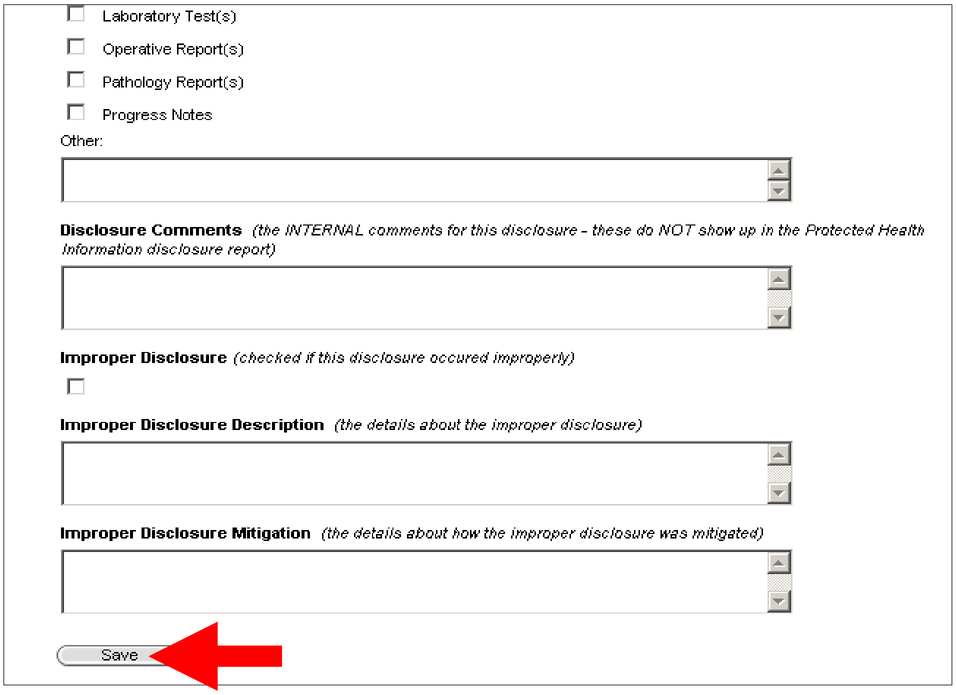
10. Select the Disclosure Status from the drop-down box.



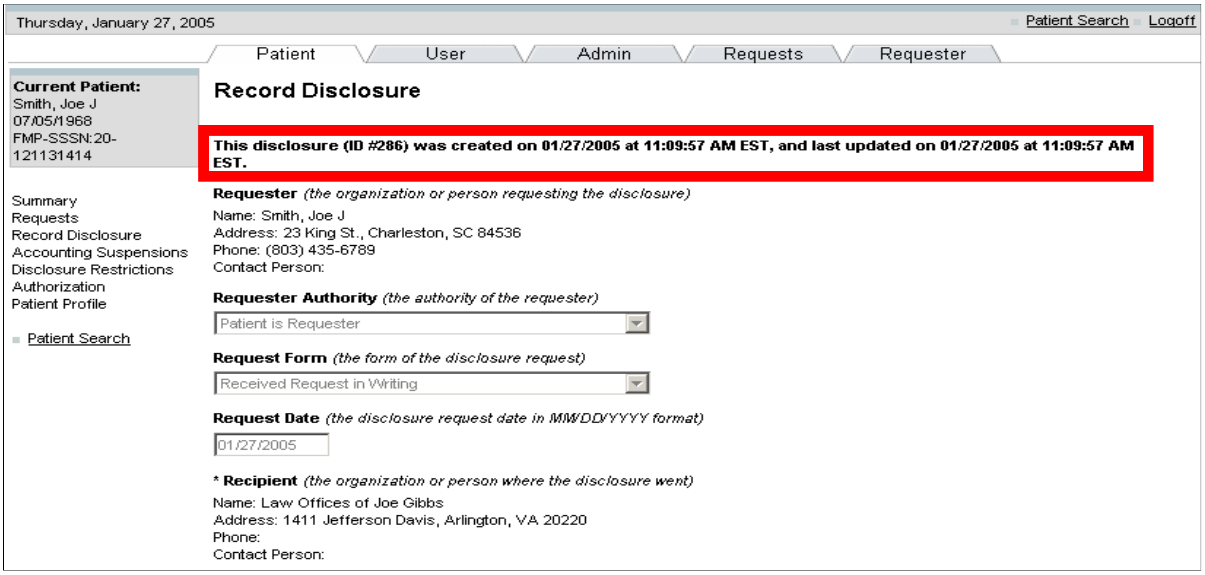
11. Scroll down the screen and enter: (disclosure date, origin organization, disclosure purpose, and PHI description).



12. Scroll down to the bottom of the screen and click on the Save button.



- The disclosure is now complete and only the disclosure comments and improper fields can be updated.



<u>NOTE:</u> To view the disclosure:

- *Select the user tab*
- *Select My Requests hyperlink*
- *The disclosure is displayed in the User Request box*
- *To view specific details of the disclosure, select the Request Session ID for that particular request*

<u>NOTE</u>: To Amend Disclosures:
Once a disclosure has a disclosure status of completed, the only way to amend it is by assigning it as an Improper Disclosure. For information on Improper Disclosures, see section 8.10 Amend Disclosures.

<u>NOTE</u>: Disclosures with Special Circumstances

When making multiple disclosures for the same patient, and for the same purpose, record all information in one disclosure record. Record the disclosure as stated in the previous steps using the following guidance.

Guidance for Completing Disclosure with Special Circumstances	
Data Field	**Data to be Provided**
Information Start Date	Provide the date for which the disclosure request begins
Information End Date	Leave blank if unknown or insert the date for one year later
Disclosure Date	Insert the date of the first disclosure
Treatment Start Date	Insert the date on which the treatment began
Treatment End Date	Leave blank
Disclosure Purpose/Other	Insert text to indicate the frequency of disclosure and the number of disclosures to be made in addition to any other pertinent information such as the name of the report it will support

If there is no end date be sure to report that there is no end date at this time and therefore the disclosure record will expire in one year. At that time, if the regular disclosures are still ongoing, then a new disclosure record will be created.

NOTE: Remember that the text entered in this field does appear on reports and correspondence generated by the PHIMT.

8.2 APPROVE DISCLOSURES

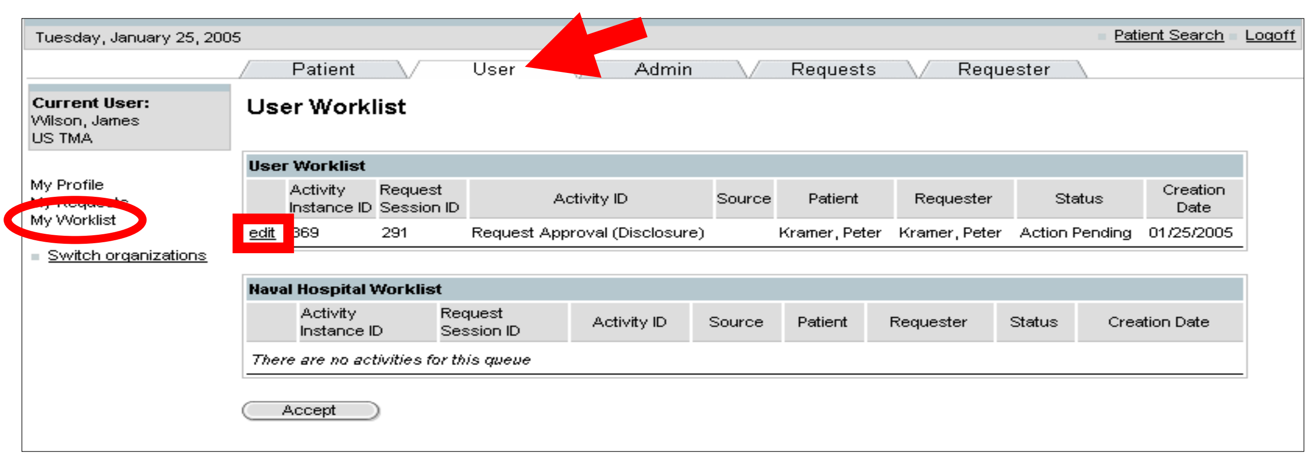
NOTE: Those disclosures recorded by you using the Record Disclosure hyperlink have already been approved. This approval activity is for those disclosures that were developed using the Record Disclosure wizard and routed to your worklist for later action.

To approve a disclosure:

1. Select the User Tab.

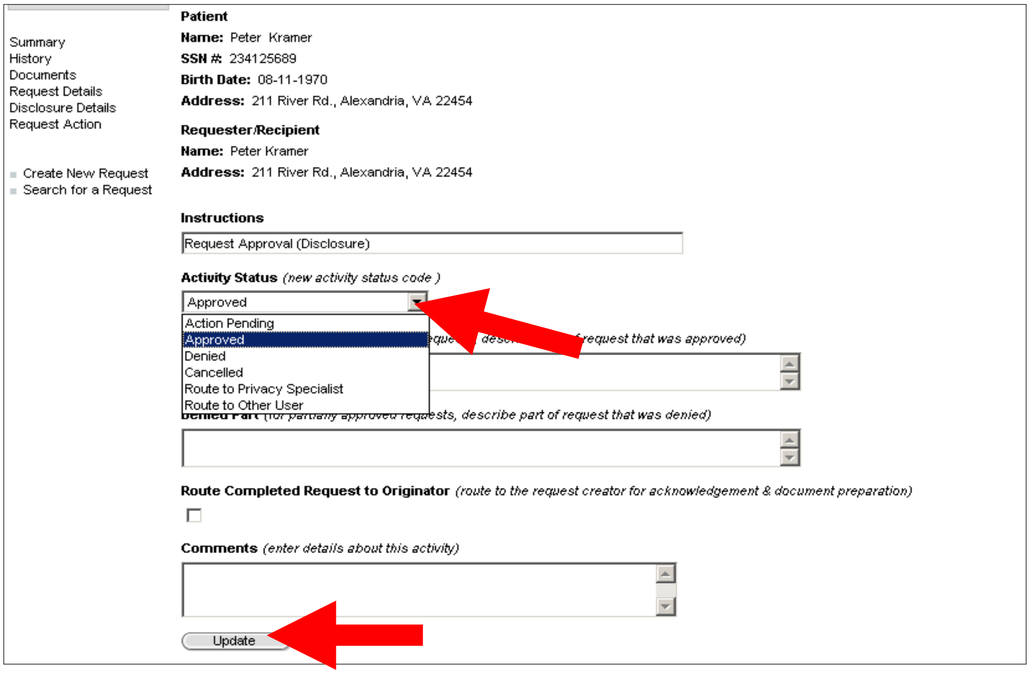
2. Select the My Worklist hyperlink.

3. Select the Edit hyperlink for the disclosure you want to approve.



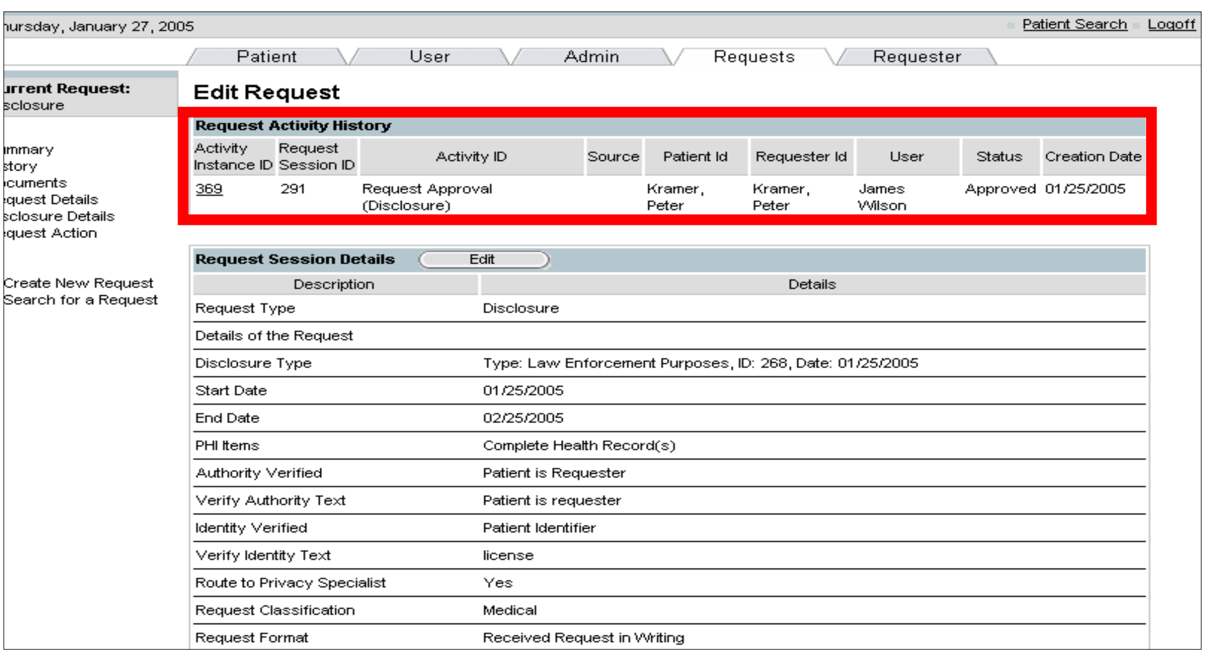
4. Select Approved from the Activity Status drop-down box.

5. Click on the Update button.



- The Edit Request screen appears. The approved request will display in the Request Activity History box. The status has been changed to Approved.

<u>NOTE</u>: The disclosure is no longer shown on your User Worklist.



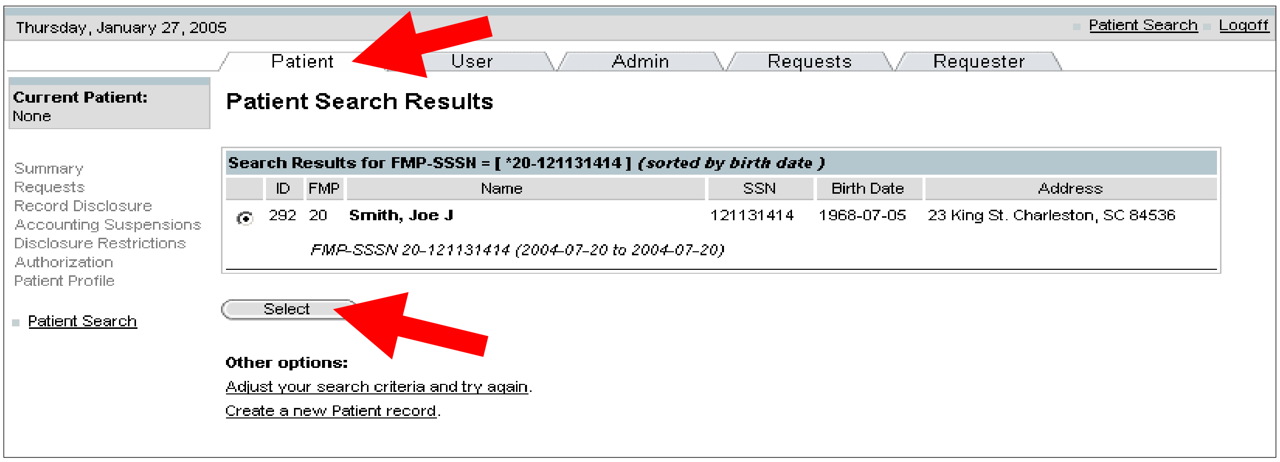
8.3 AMEND A DISCLOSURE

As a Privacy Specialist you are authorized to label a disclosure as Improper. Once a Disclosure status is marked as completed, it can only be amended by marking it as an Improper Disclosure, which means the disclosure was made incorrectly.

To amend a disclosure:

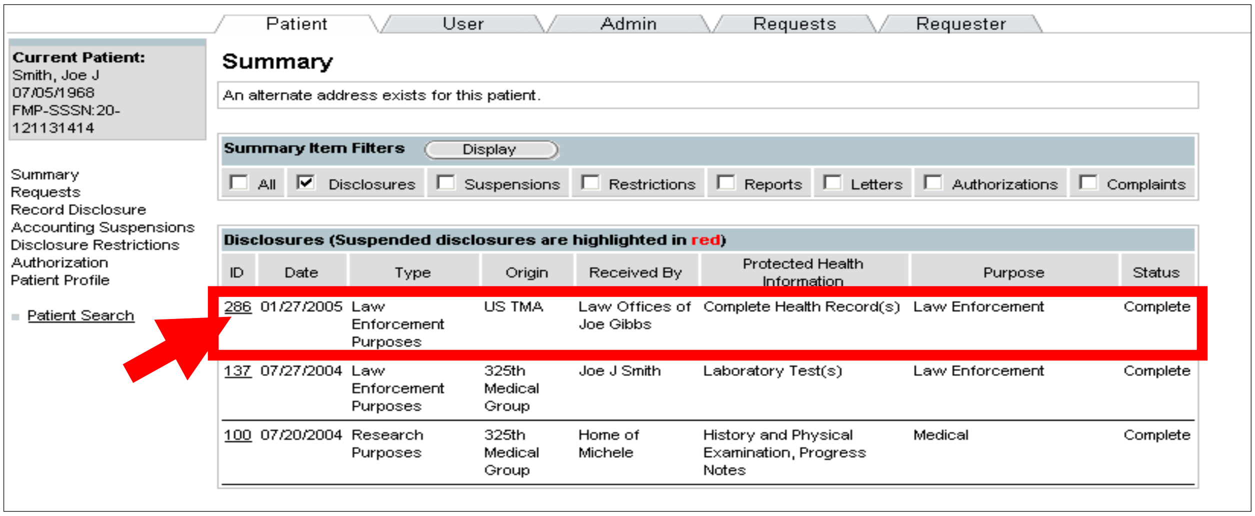
1. Select the Patient Tab.

2. Search for and select the patient.

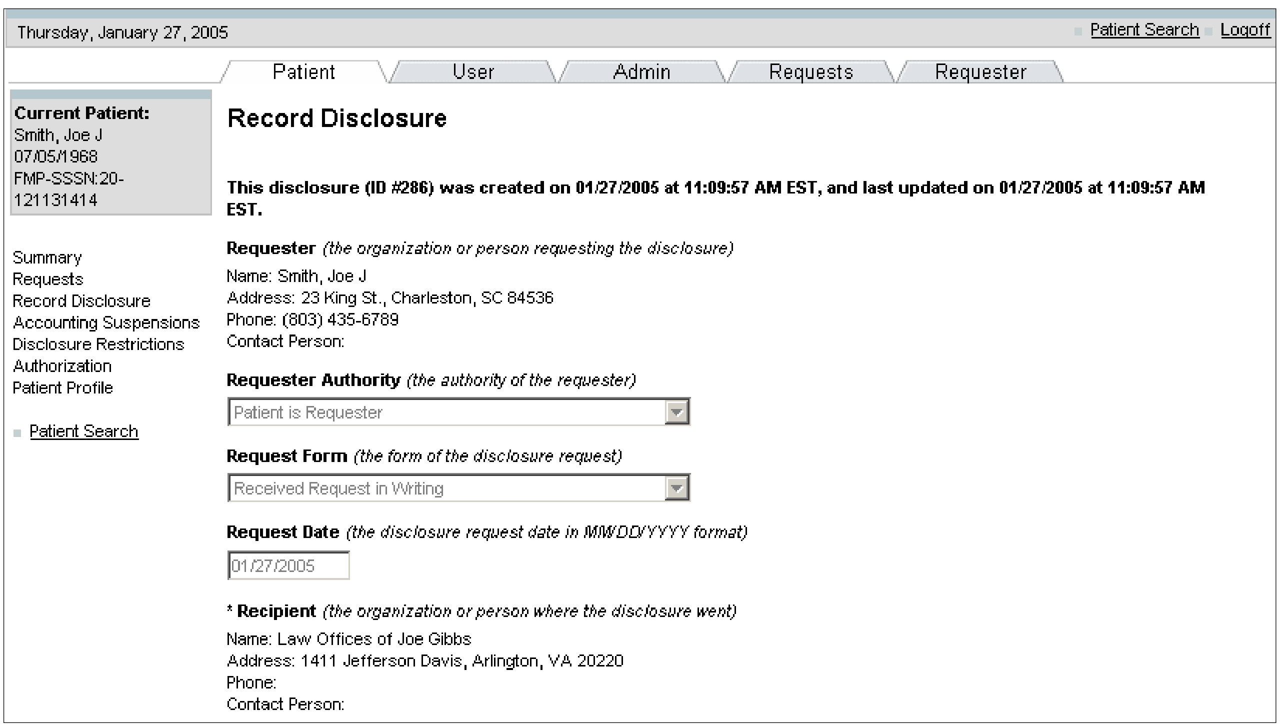


3. Place a check in the Disclosures box and click on the Display button.

4. Select the ID hyperlink for the disclosure that you want to amend.



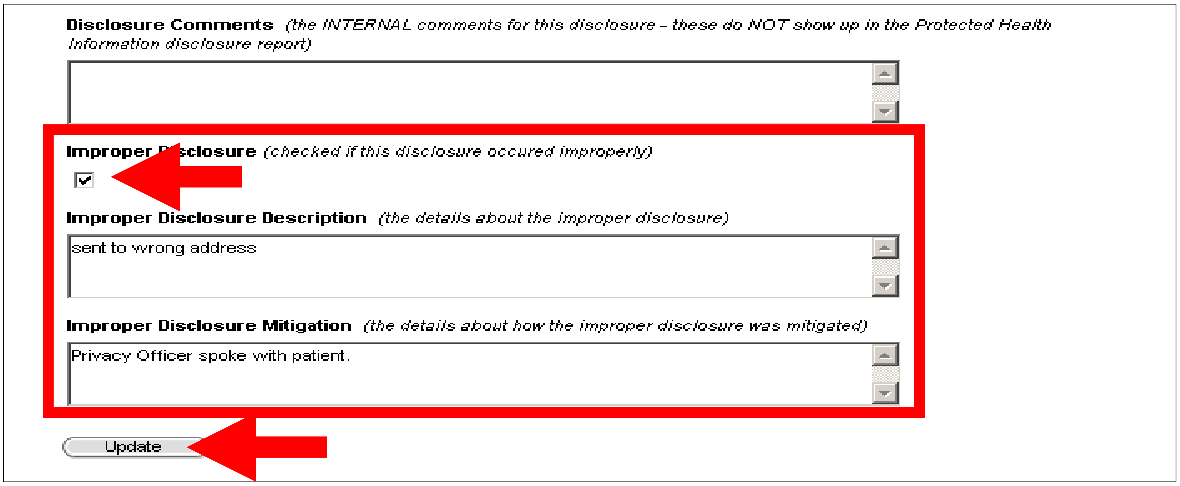
- The Record Disclosure screen will display.



5. Scroll to the bottom of the screen and place a check in the Improper Disclosure checkbox.

6. Enter a description of the Improper Disclosure and mitigation.

7. Click on the Update button.



8.4 RECORD A REQUEST FOR AN ACCOUNTING OF DISCLOSURES

An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the 6 years prior to the date that the accounting is requested– DoD 6025.18-R Chapter 13.

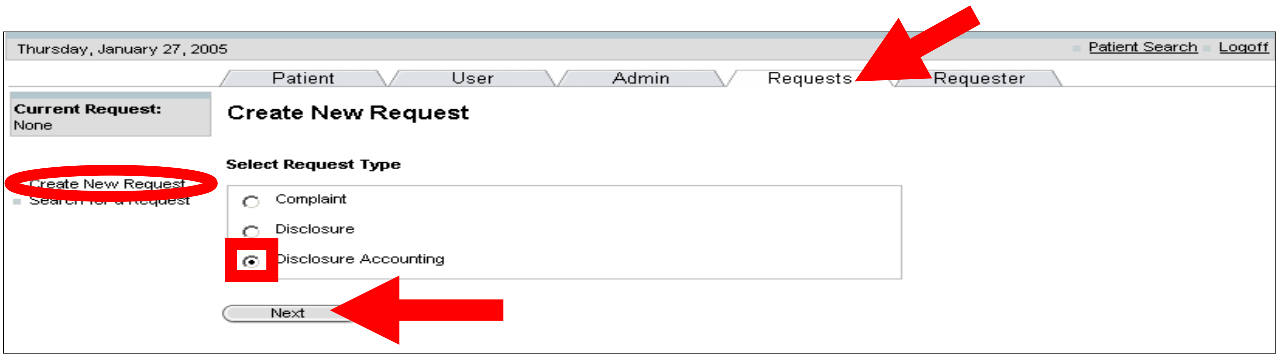
Both Regular Users and Privacy Specialists can record a request for an accounting of disclosures, but only Privacy Specialists can approve or deny the request.

To record a request for an accounting of disclosures:

1. Select the Requests Tab.

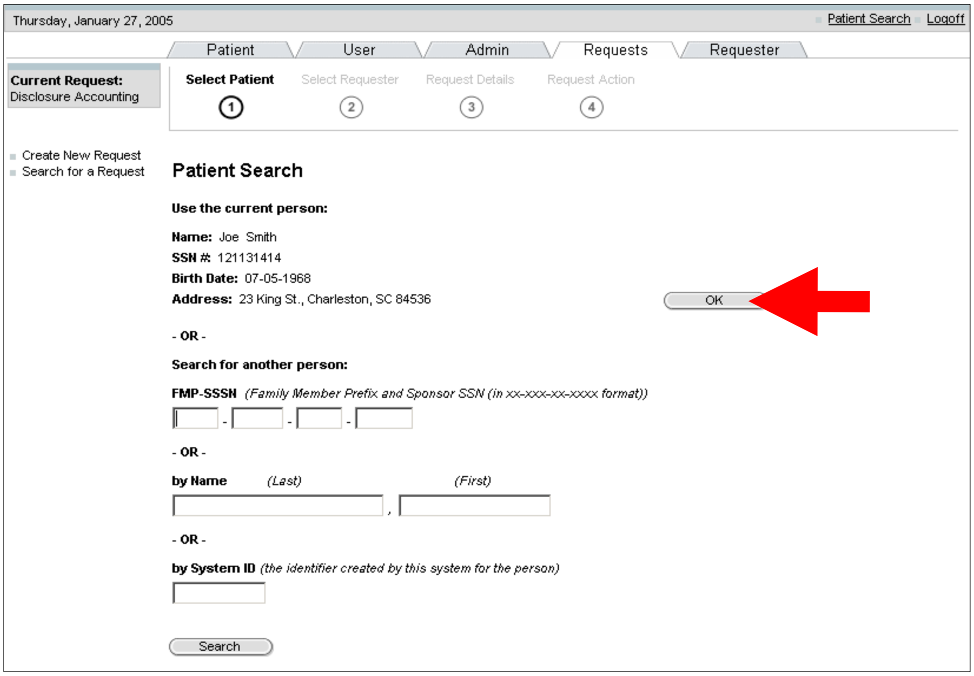
2. Select the Create New Request hyperlink and/or click on the radio button for Disclosure Accounting.

3. Click on the Next button.

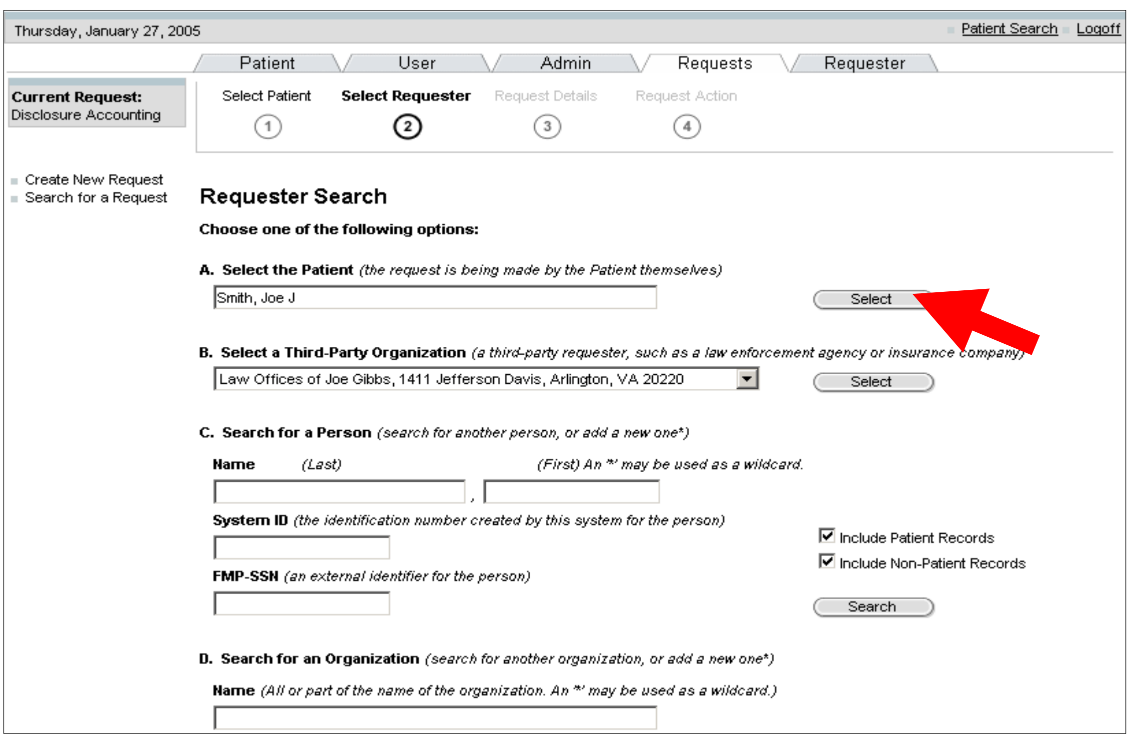


4. Search for or select the patient.

5. Click on the OK button.

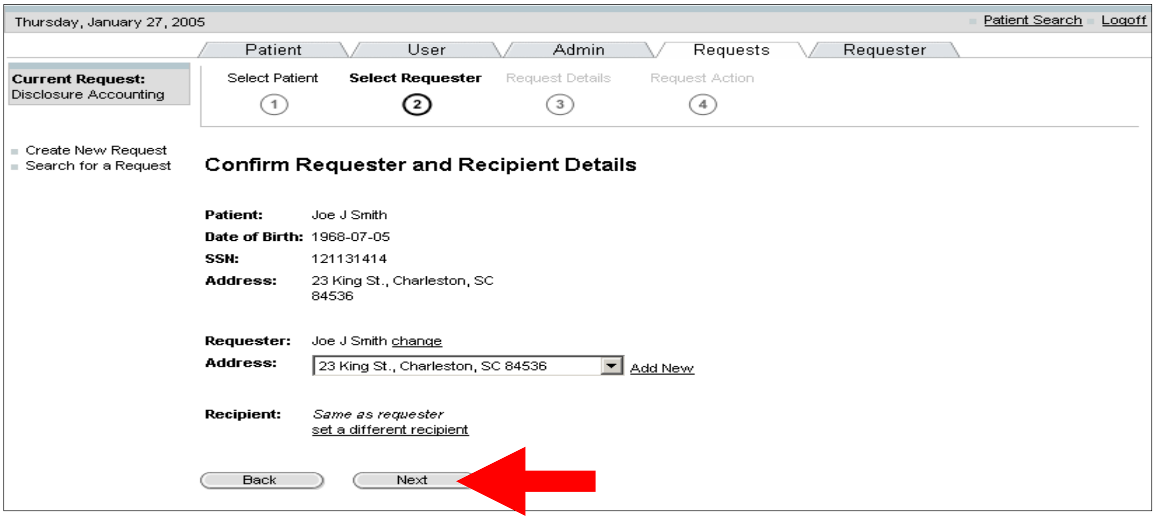


6. Select the Requester.



7. Confirm the requester and recipient details.

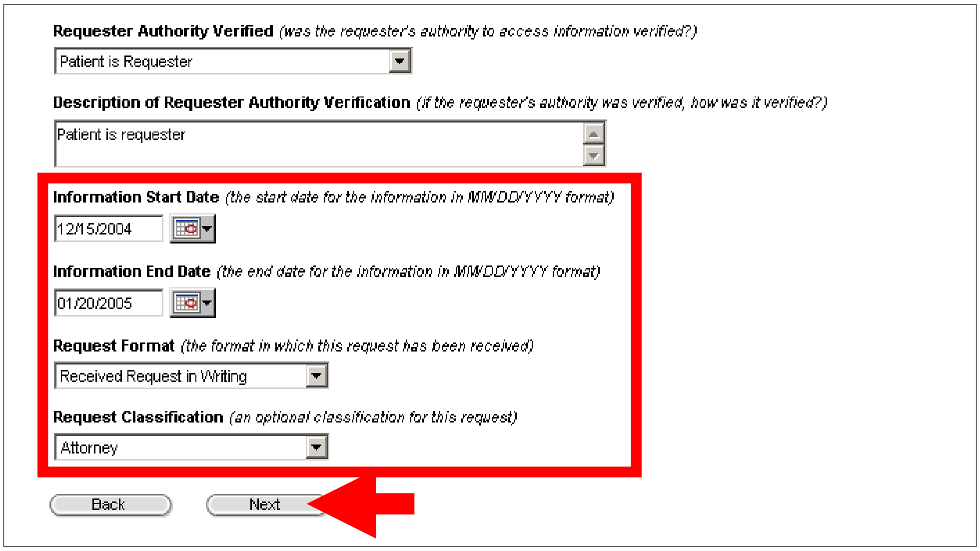
8. Click on the Next button.



9. Enter the Request Details: (details of the request, identity verification, authority verification).

10. Scroll down the screen and enter: (Information start and end date, request format, and request classification).

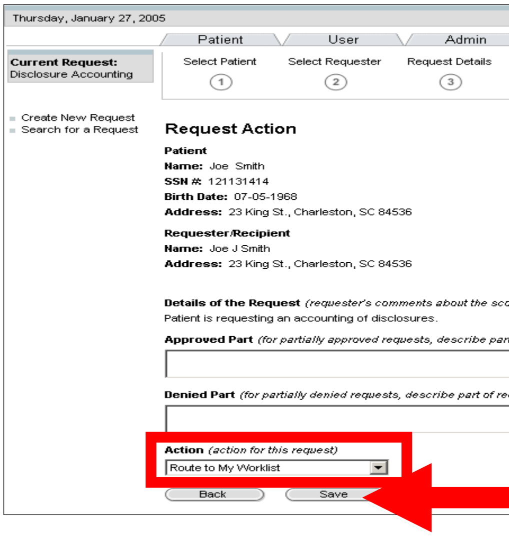
11. Click on the Next button.



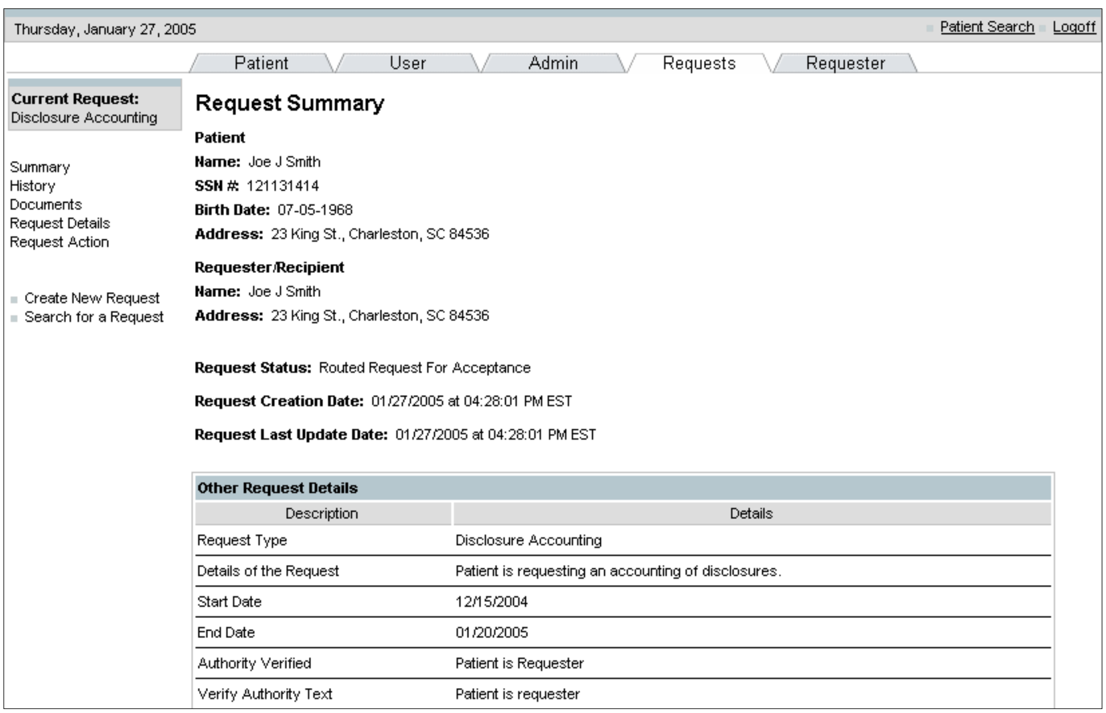
12. Enter in the Request Action Details.

13. From the Action Drop-down box, select the appropriate person to route the request to.

14. Click on the Save button.



- The Request Summary screen will display.



8.5 APPROVE ACCOUNTING OF DISCLOSURES

A patient may ask for an Accounting of Disclosures at any time. PHIMT allows for a quick reporting of this accounting.

The Request Action window provides you with various accounting disclosure actions, which are shown in this table:

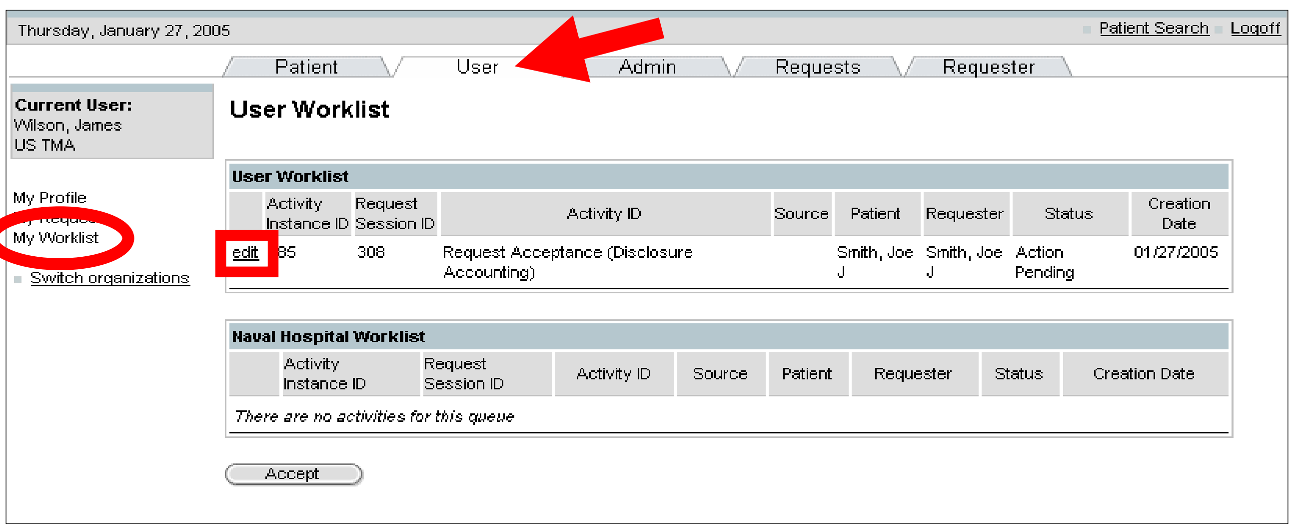
Accounting for Disclosures - Request Actions	
Action	**Description**
Route to My Worklist	Allows you to place it on your worklist to follow up when appropriate
Process Request Now	Allows you to place it in your worklist for approval
Deny Request Now	Allows you to deny the disclosure
Route to Privacy Specialist	Allows you to pass the disclosure on to another Privacy Specialist to be processed, as established in a User-to-User Relationship
Route to Other User	Allows you to pass the disclosure back to another user to process the letter generation after approving or denying the request, as established in a User-to-User Relationship

To approve an accounting of a disclosure:

1. Select the User Tab.

2. Select the My Worklist hyperlink.

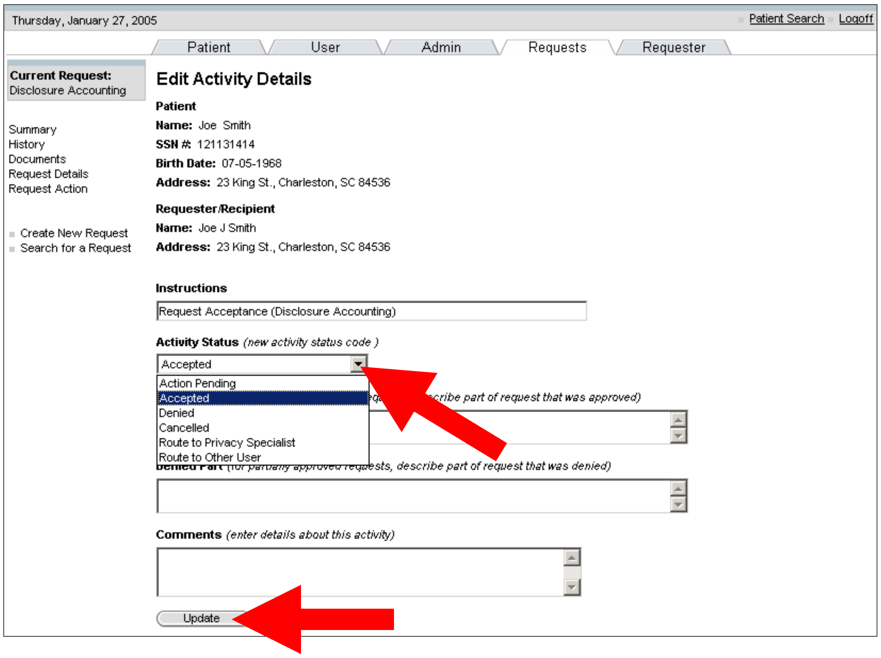
3. Select the Edit hyperlink for the disclosure accounting that you want to approve.



- The Edit Activity Details screen will display.

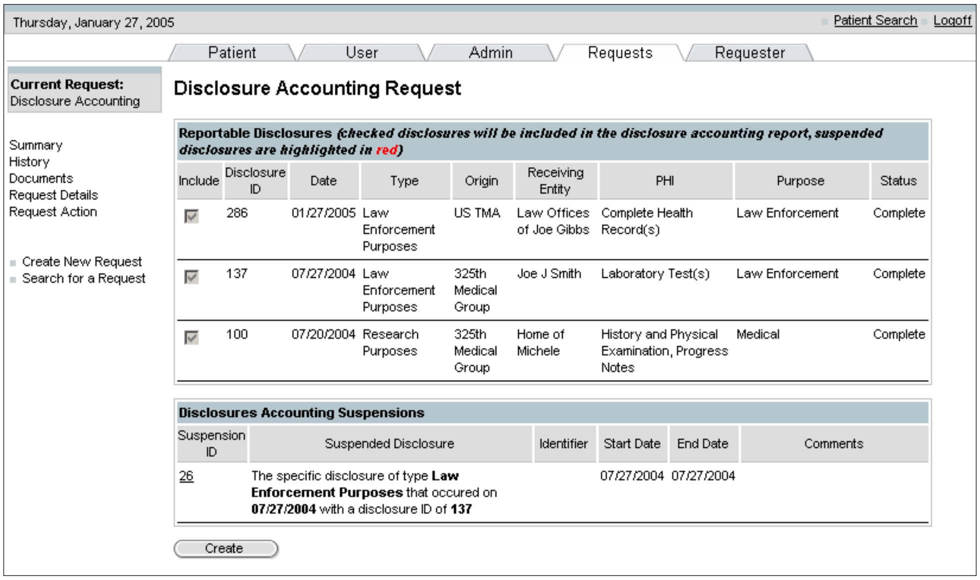
4. Select Accepted from the Activity Status drop-down box.

5. Click on the Update button.



- The Disclosure Accounting Request screen will display with the approved accounting of disclosures.

  NOTE: The accounting disclosure (Activity Instance ID 76) is no longer shown on your User Worklist



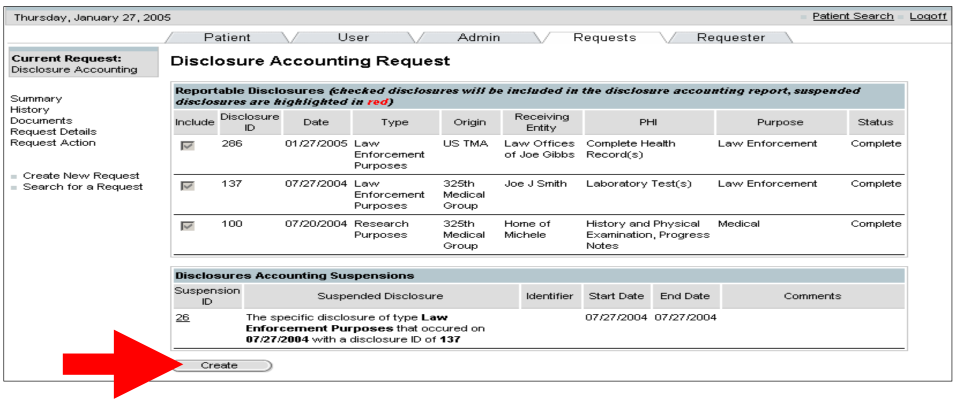
8.6 GENERATE AN ACCOUNTING OF DISCLOSURES REPORT

An accounting of disclosures report is a summary of all of the disclosures made for a particular patient. Once a request has been approved, an accounting of disclosures report can be generated.

The Privacy Specialist has the option to route the report back to the originator. Pending disclosures will not display in the report.

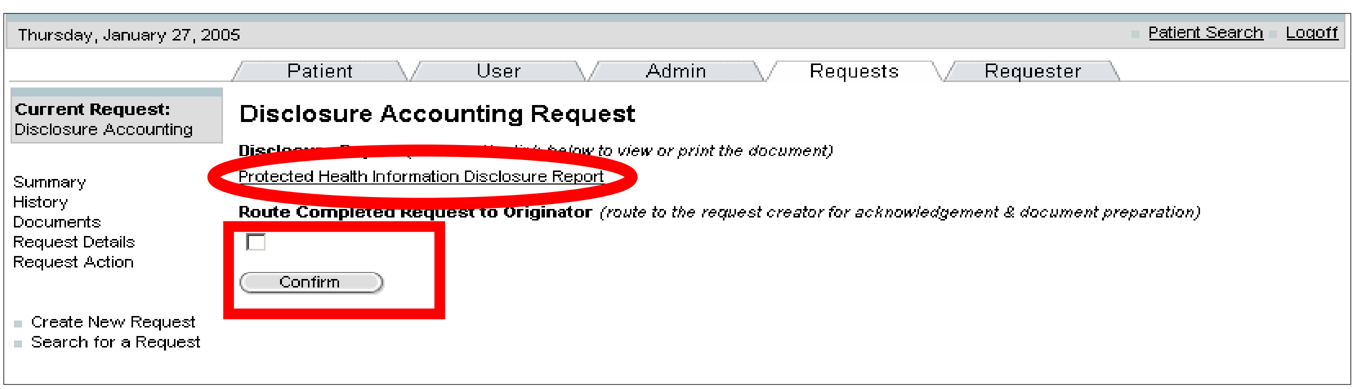
To generate an Accounting of Disclosures Report:

1. From the Disclosure Accounting Request screen, click on the Create button to generate the report.

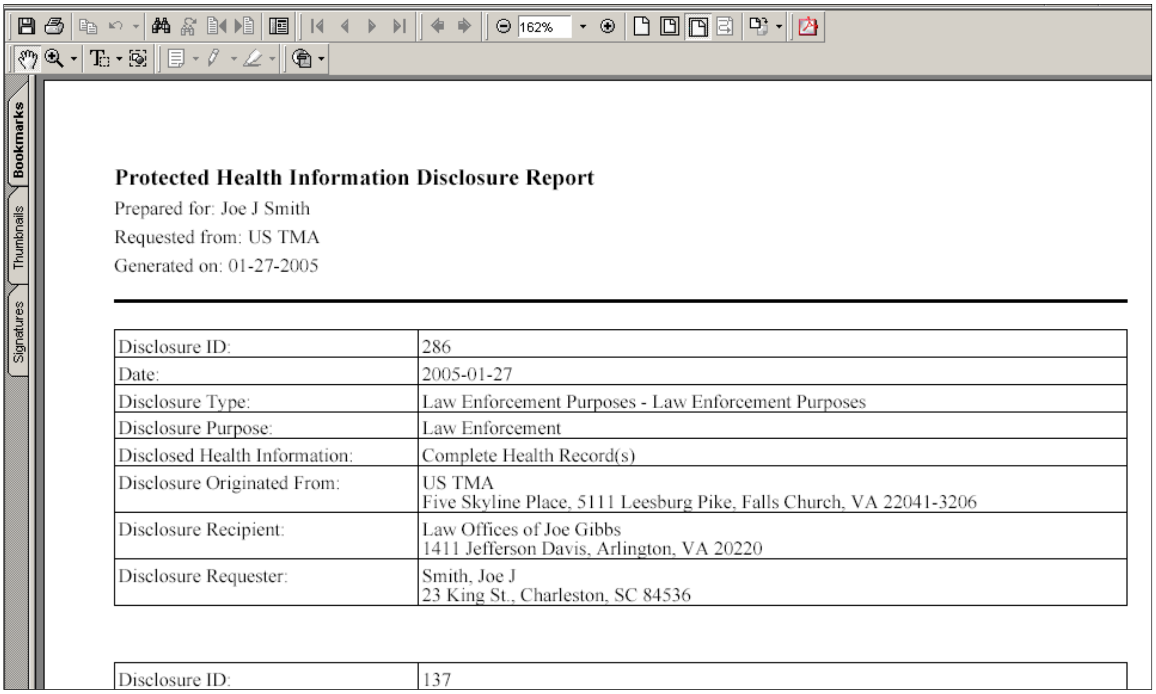


2. Select the Protected Health Information Disclosure hyperlink to create the report.

<u>NOTE:</u> If you want to route the completed request back to the originator, place a check in the box and click on Confirm.



3. The Accounting of Disclosures Report will display.



Protected Health Information Disclosure Report
Prepared for: Joe J Smith
Requested from: US TMA
Generated on: 01-27-2005

Disclosure ID:	286
Date:	2005-01-27
Disclosure Type:	Law Enforcement Purposes - Law Enforcement Purposes
Disclosure Purpose:	Law Enforcement
Disclosed Health Information:	Complete Health Record(s)
Disclosure Originated From:	US TMA Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Disclosure Recipient:	Law Offices of Joe Gibbs 1411 Jefferson Davis, Arlington, VA 20220
Disclosure Requester:	Smith, Joe J 23 King St., Charleston, SC 84536

Disclosure ID:	137

8.7 CREATE A SUSPENSION

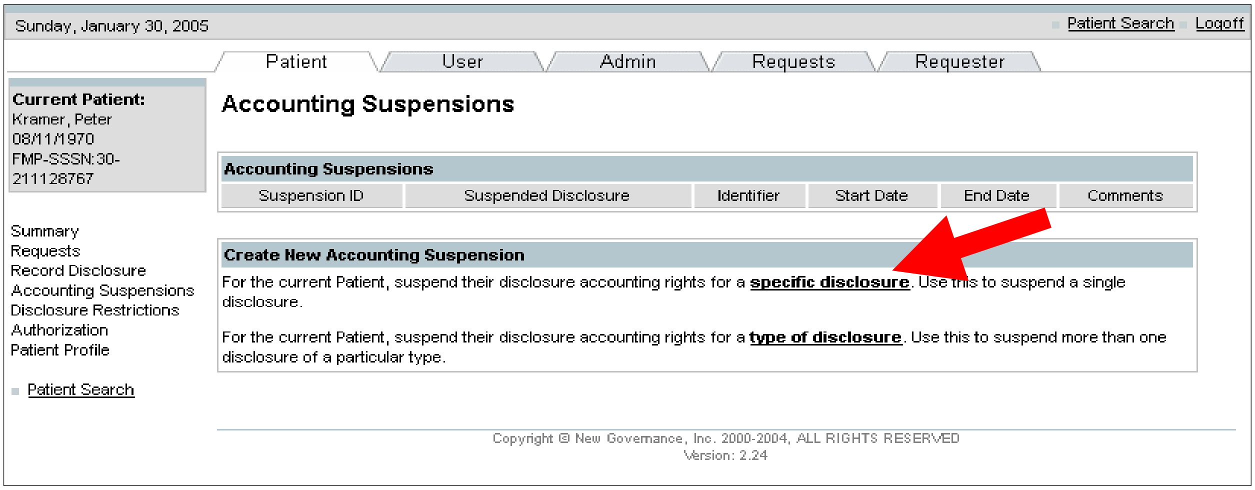
The covered entity shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official…DoD 6025.18-R C13.1.2.1 Two types of disclosures can be suspended: Law enforcement purposes and Health oversight activities. Privacy Specialists have the ability to enter an accounting suspension in two ways: Specific disclosure and Type of disclosure. As a best practice, it is recommended that users enter in an accounting suspension using the Specific disclosure hyperlink. Once a suspension has been entered, all users can view it.

To create a suspension:

1. Search for and select a patient record.

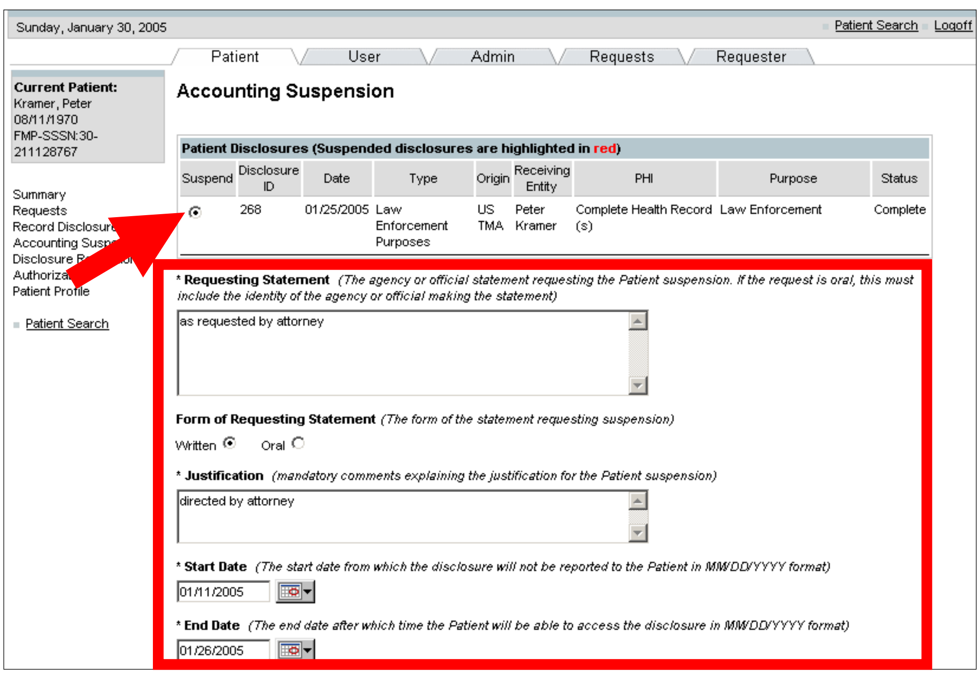
2. Select the Accounting Suspensions hyperlink.

3. Select the Specific Disclosure hyperlink.

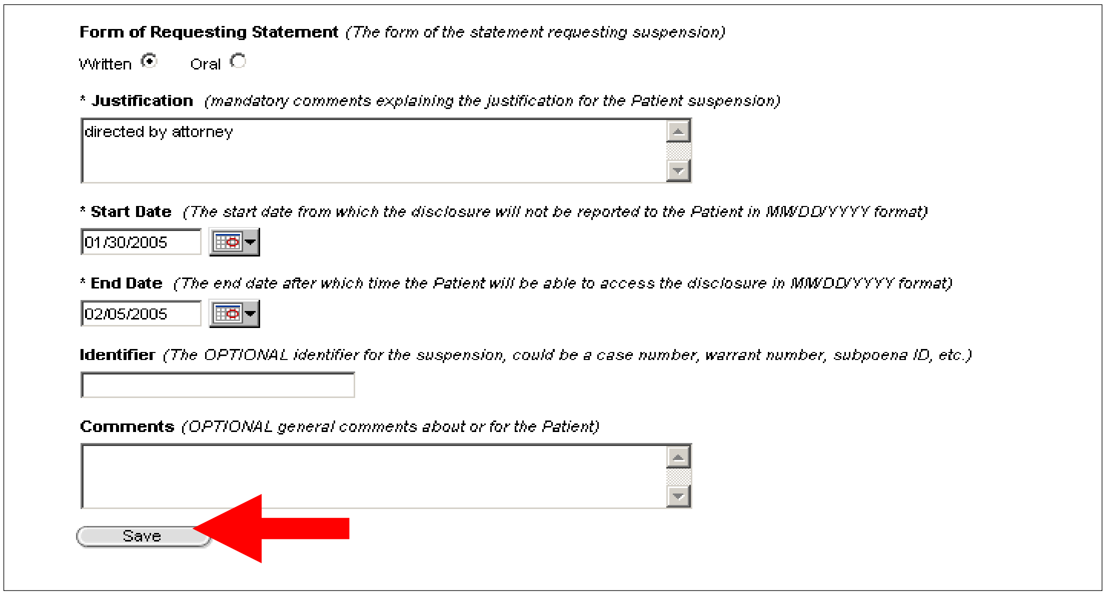


4. Click on the radio button for the disclosure you want to suspend.

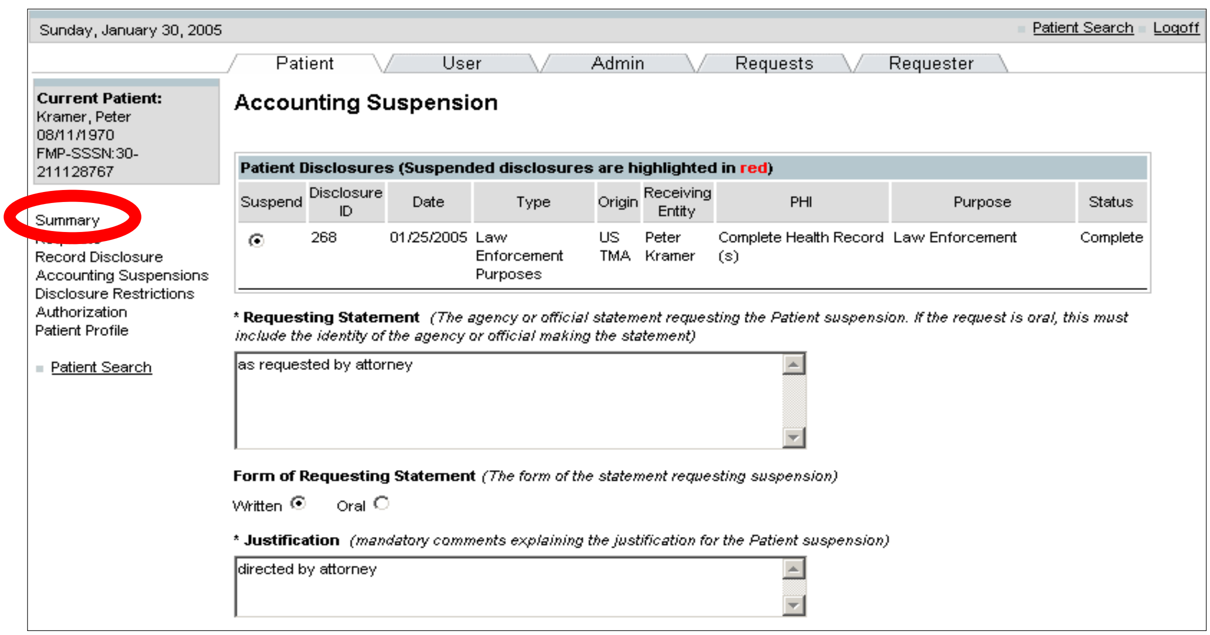
5. Enter the suspension details: (requesting statement and form, justification, and start and end date).



6. Scroll to the bottom of the screen and click on the Save button.



7. Select the Summary hyperlink.



8. Check the Suspensions checkbox.

9. Click on the Display button.

- The Disclosure that you suspended will display in the Disclosure Accounting Suspensions section.

8.8 RECORD COMPLAINTS

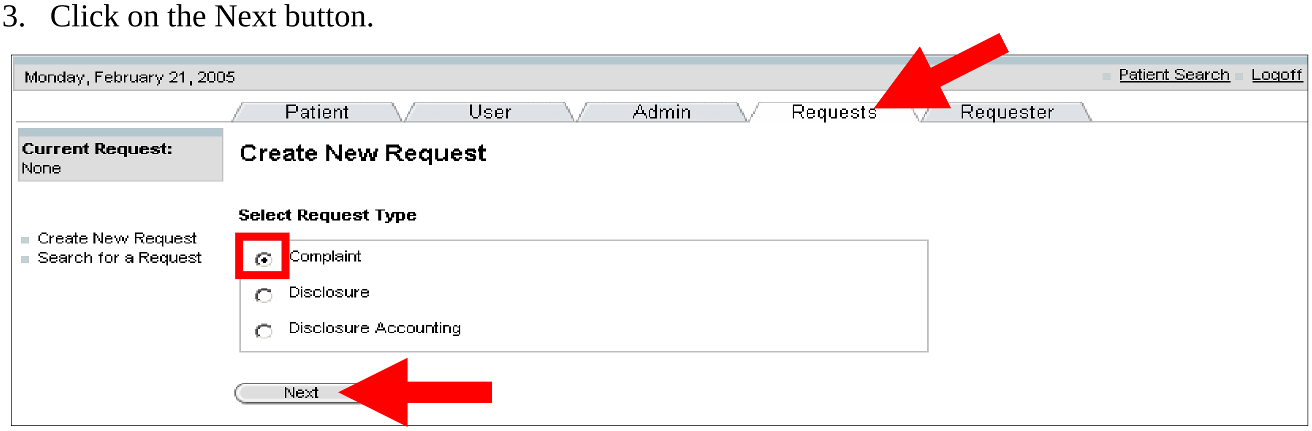
NOTE: The Record Complaint is performed on the Requests tab and has three steps: select complainant, complaint details, and request action.

To record a complaint:

1. Select the Requests Tab.

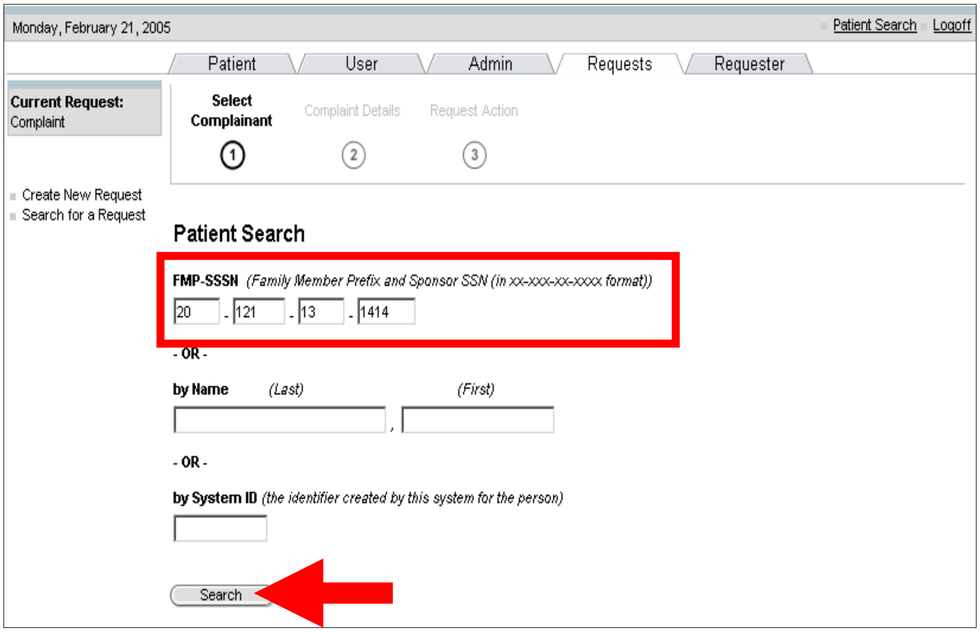
2. Select Complaint in the Select Request Type box.

3. Click on the Next button.

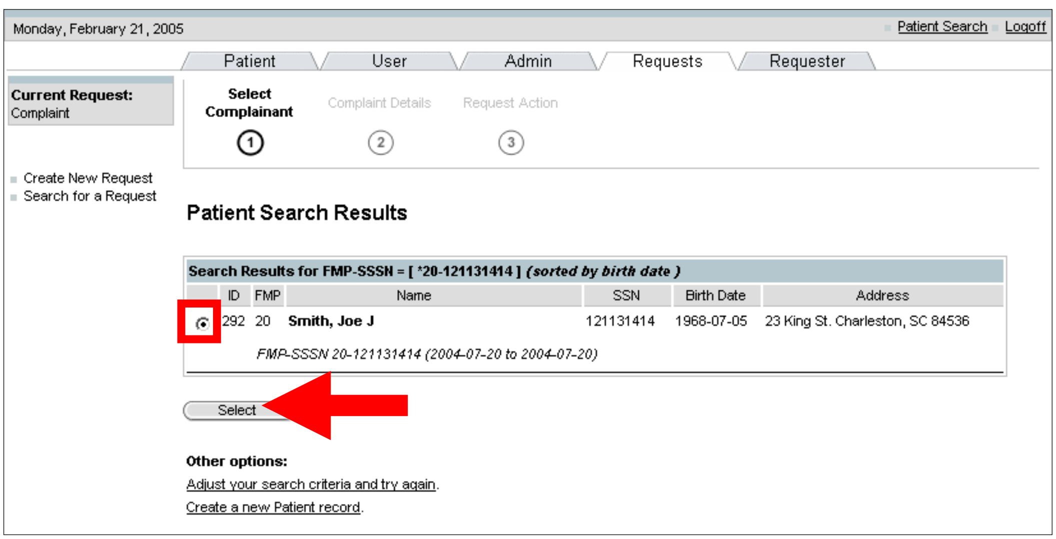


4. Type in the name of the person making the complaint or their FMP-SSSN.

5. Click on the Search button.



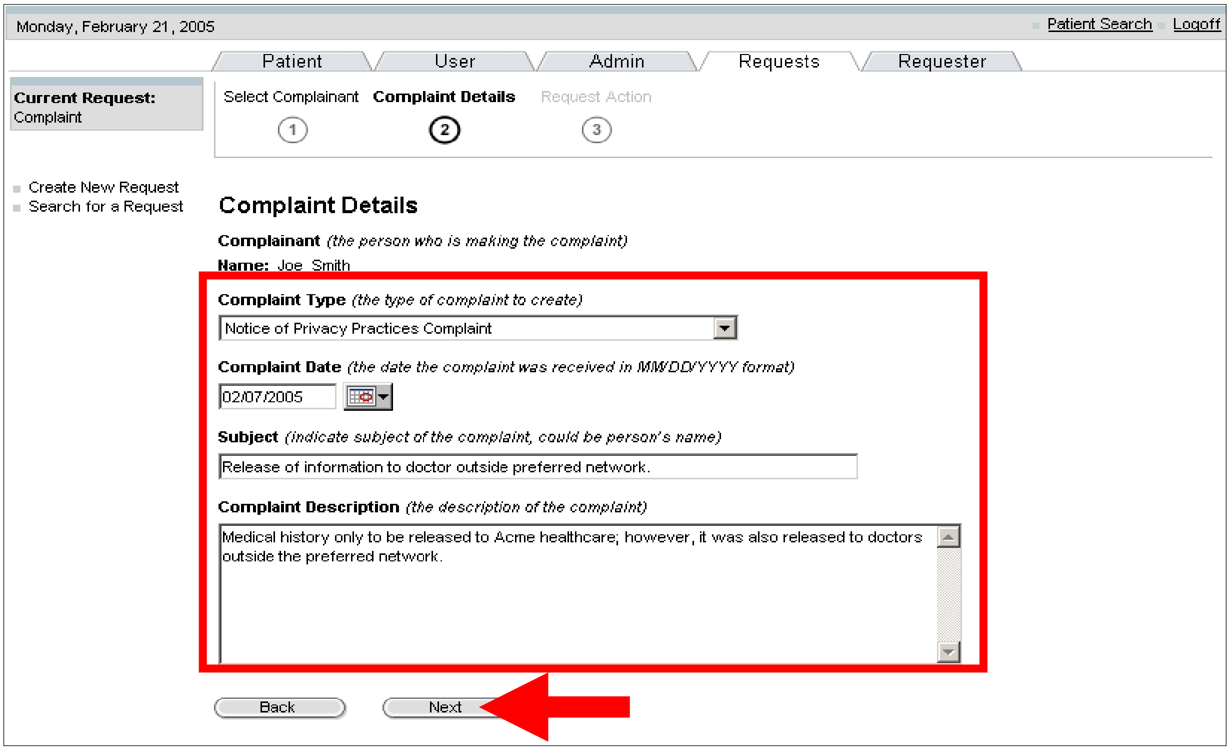
6. Select the person from the Patient Search Results screen.



- The Complaint Details screen appears.

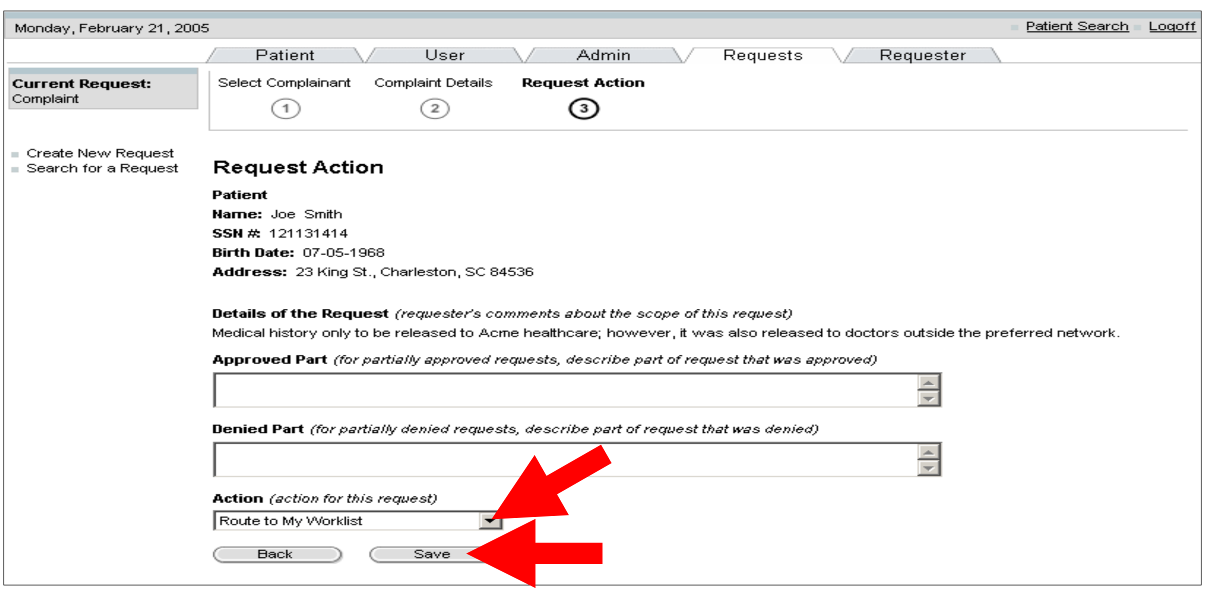
7. Provide the required information: (complaint type, complaint date, the subject and description of the complaint).

8. Click on the Next button.



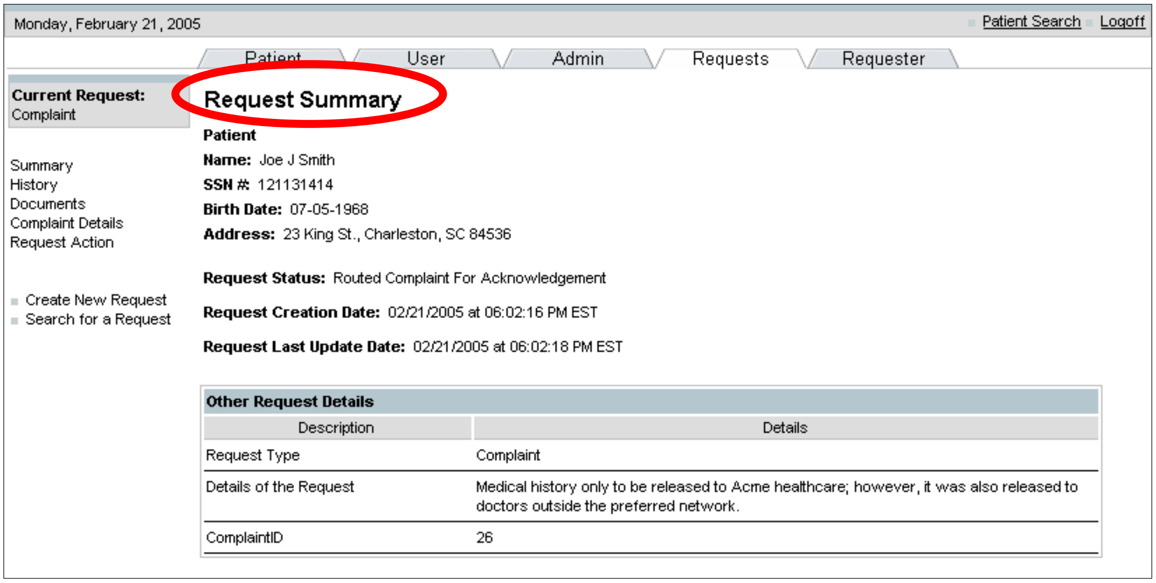
9. Select the action to be taken.

10. Click on the Save button.



- The Request Summary screen appears.

- The details of the complaint are displayed on the Request Summary screen.



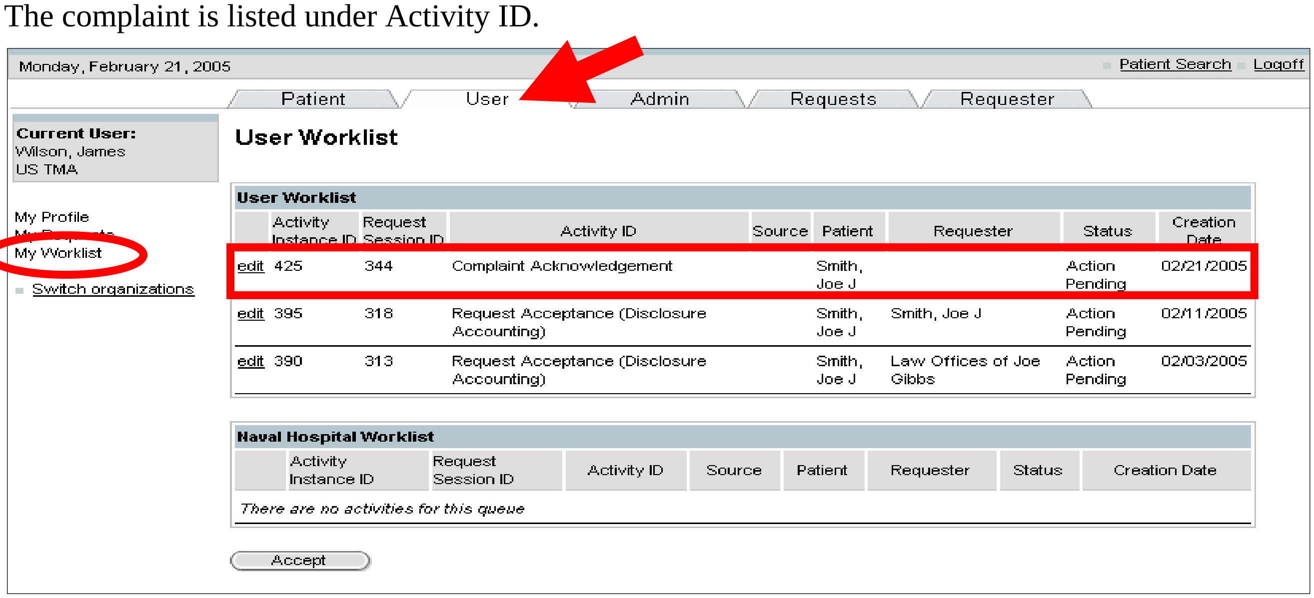
<u>NOTE</u>: The complaint is displayed on your worklist.

To view the complaint:

1. Select the User Tab.

2. Select the My Worklist hyperlink.

The complaint is listed under Activity ID.



<u>NOTE</u>: You can also view a summary of the complaint.

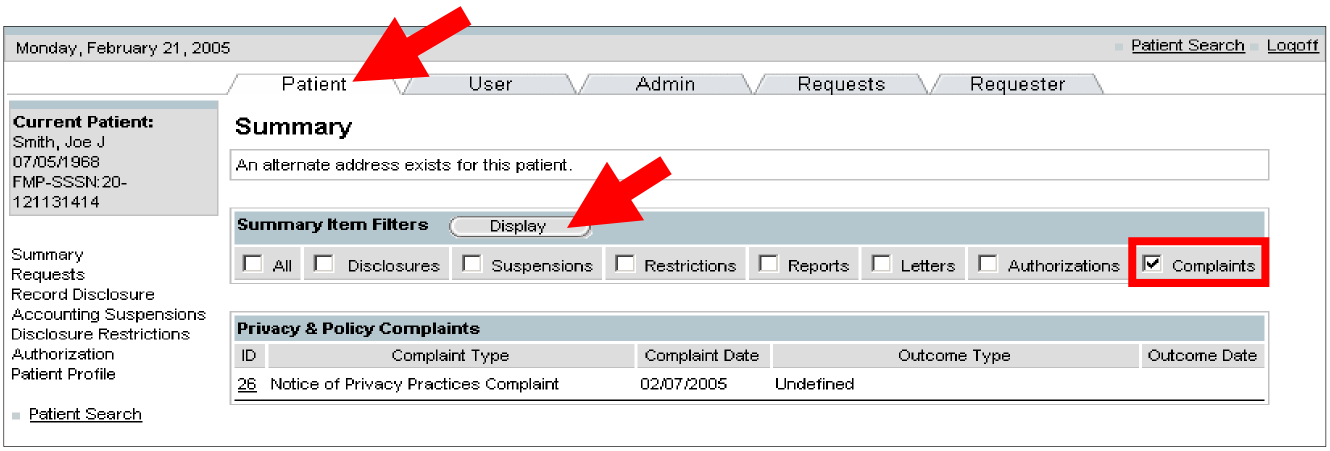
To view a summary of the complaint:

1. Select the Patient Tab.

2. Select the Complaints box.

3. Click on the Display button.

The Patient Summary screen displays the type of complaint action.



8.9 RECORD DISCLOSURE RESTRICTIONS

As a Privacy Specialist you are able to enter a Restriction of Disclosure or terminate a Restriction of Disclosure. Restriction of Disclosures allows members to restrict uses and disclosure of their PHI.

When selecting the Disclosure Type if you determine that you need a new type of disclosure, contact the HIPAA Support Center.

NOTE: Ensure that you enter specific details of what information is being restricted. It is important to be specific in this entry because it will provide other staff members with the details about the individual and organization, and about the restrictions on the disclosure.

To record a disclosure restriction:

1. Search for and select a patient record.

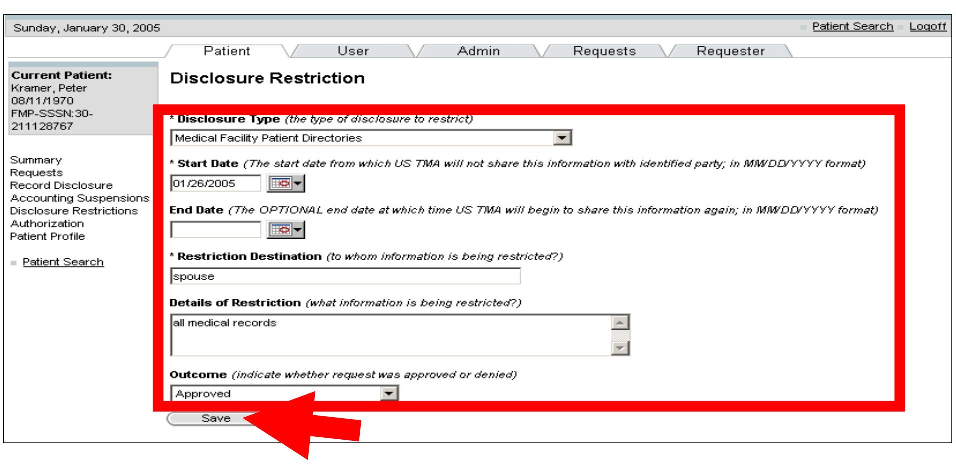
2. Select the Disclosure Restrictions hyperlink.

3. Click on the New button in the Disclosures Restrictions box.

4. Enter the Disclosure Restriction details: (disclosure type, start and end date, restriction destination (to whom information is being restricted) and details).

5. Select Approved or Denied from the Outcome drop-down box.

6. Click on the Save button.

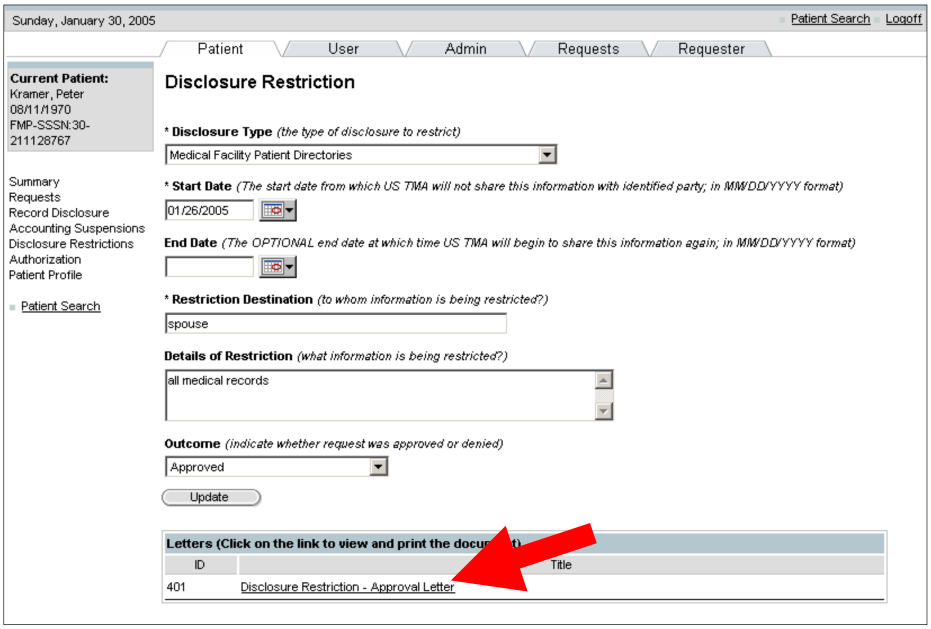


- The Patient Disclosure Restriction screen re-appears with your information. Save has changed to Update.

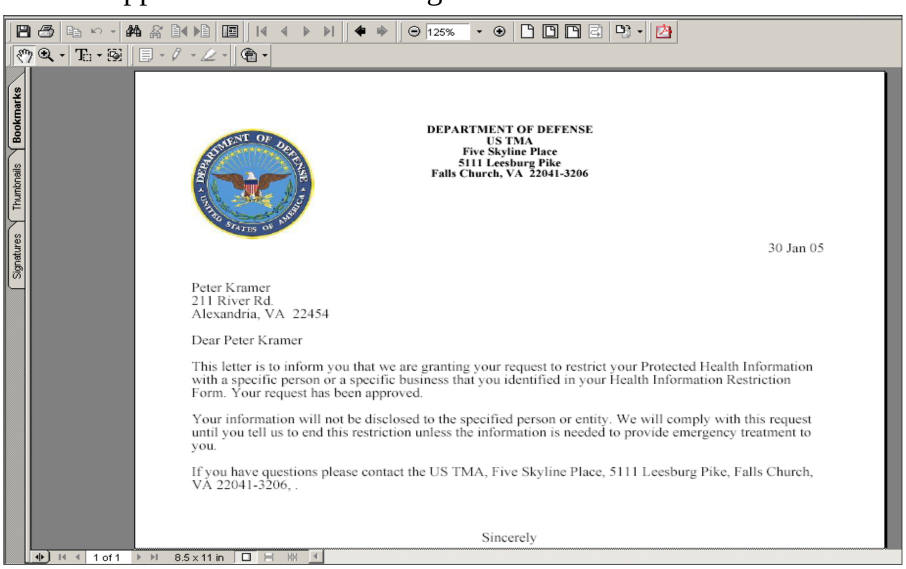
Once you have approved or denied the disclosure restriction you have the ability to generate an approval or denial letter. The letter will be pre-populated with the information that you entered for that particular restriction.

To print the Approval or Denial Letter:

1. Select the title of the letter in the Letters box on the Patient Disclosure Restriction screen.



- The Approval/Denial letter is generated.



8.10 GENERATE AUTHORIZATIONS

Record an Authorization by the patient when there is an exchange of PHI that occurs outside of the treatment, payment, or healthcare options.

Select Type of authorization. *NOTE: Based on the Type selected, the following fields are populated; however that data can be changed.*

Enter PHI to be released as it was entered on the authorization form. *NOTE: The greater the detail that is provided by the patient, the easier it will be to respond to the request at the time of disclosure.*

NOTE: Enter either the Authorization Expiration or an Action Completed date; not both. If there is no expiration date, then enter text in the Action Completed field (ex. Authorization to remain in effect until revoked.)

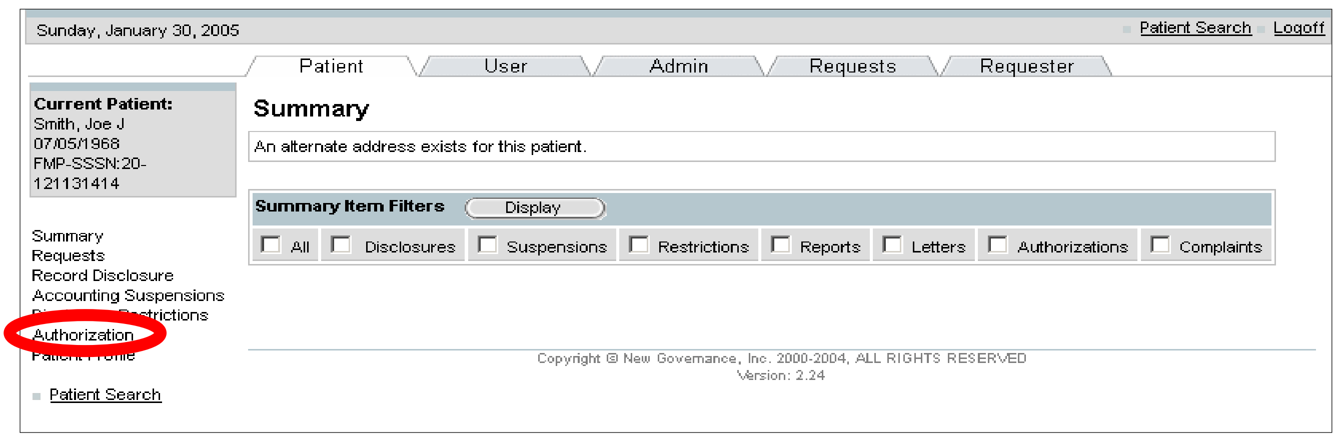
NOTE: Once the authorization has been manually signed you can go back into the particular authorization and select the Signed checkbox and enter the date of the signature using MM/DD/YYYY format or the calendar icon to select a date.

To generate an authorization:

1. Select the Patient Tab.

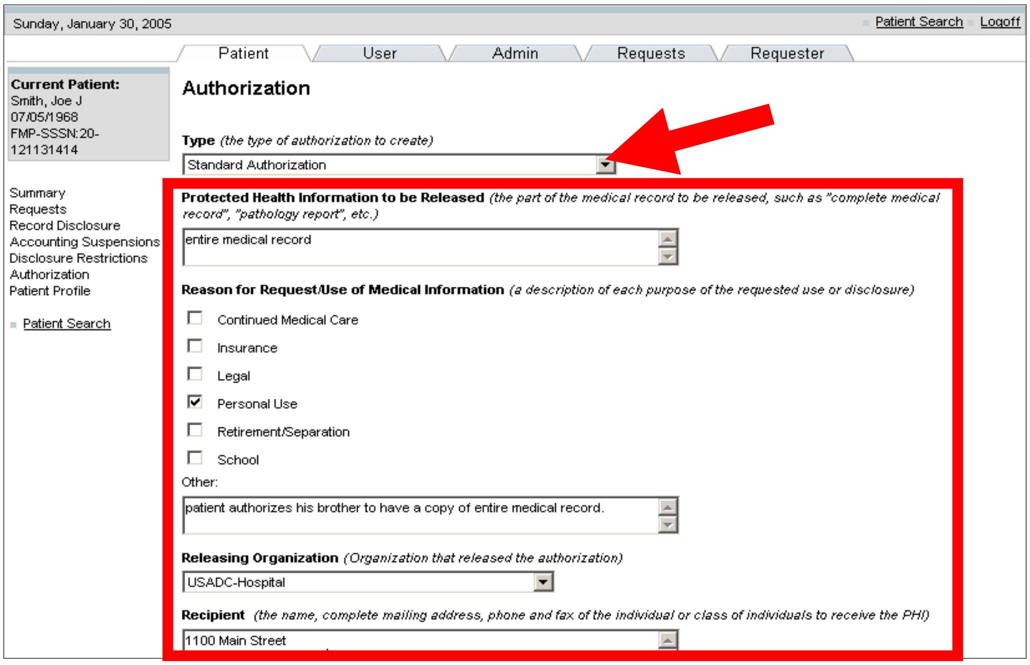
2. Search for and select the patient record.

3. Select the Authorization hyperlink.



4. Select the Authorization Type from the drop-down box.

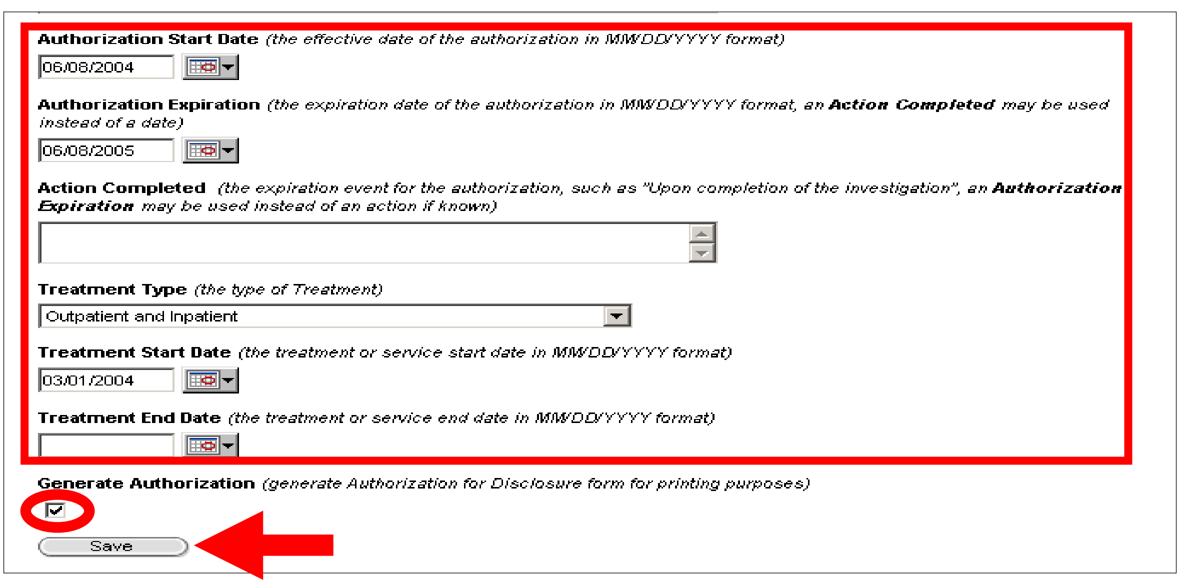
5. Enter the Authorization Details: (reason for request, releasing organization, and recipient).



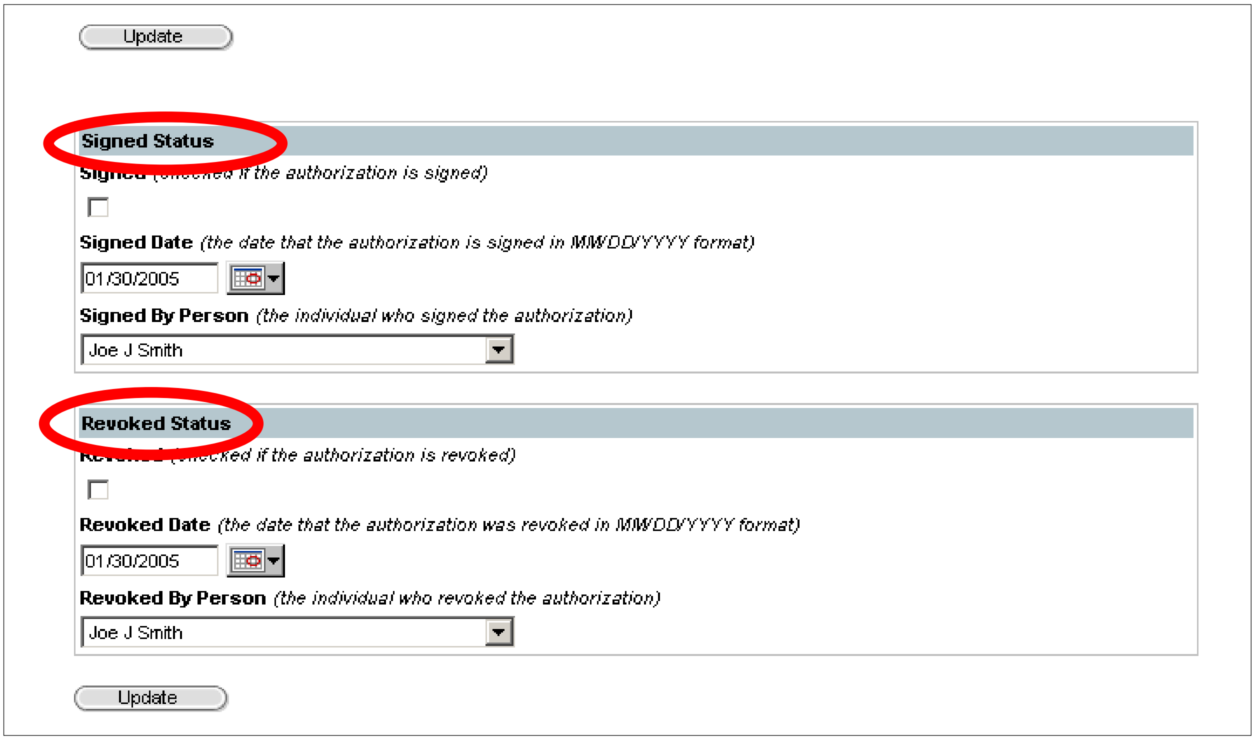
6. Scroll down the screen and enter: (authorization start and expiration date, treatment type, and treatment start and end date).

7. Place a check in the Generate Authorization checkbox.

8. Click on the Save button.

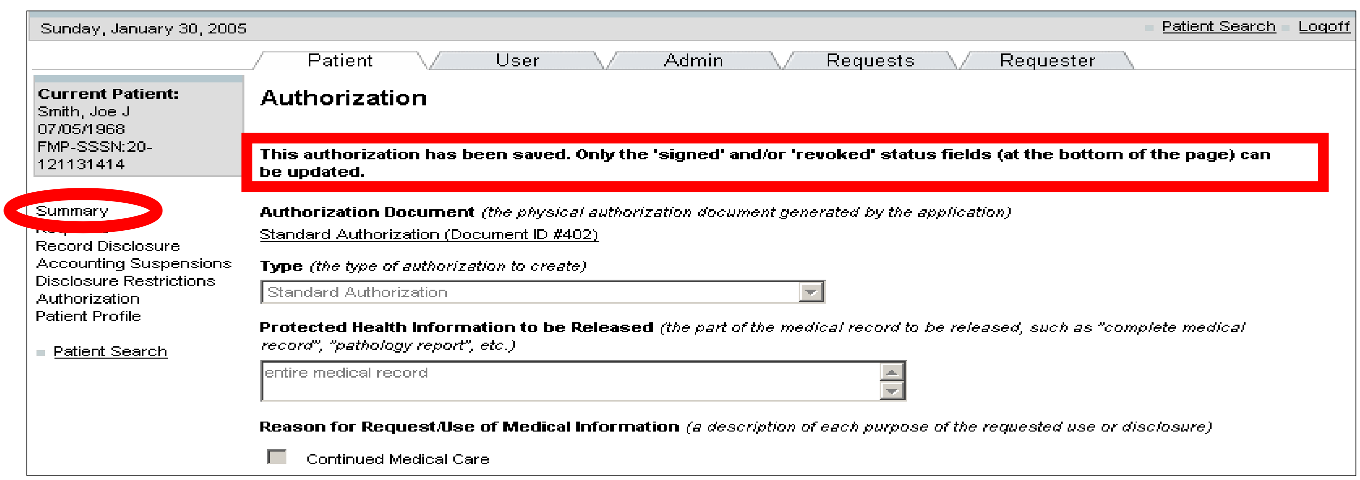


- The Signed Status and Revoked Status boxes on this screen indicate if the DD Form 2870 is signed or revoked.



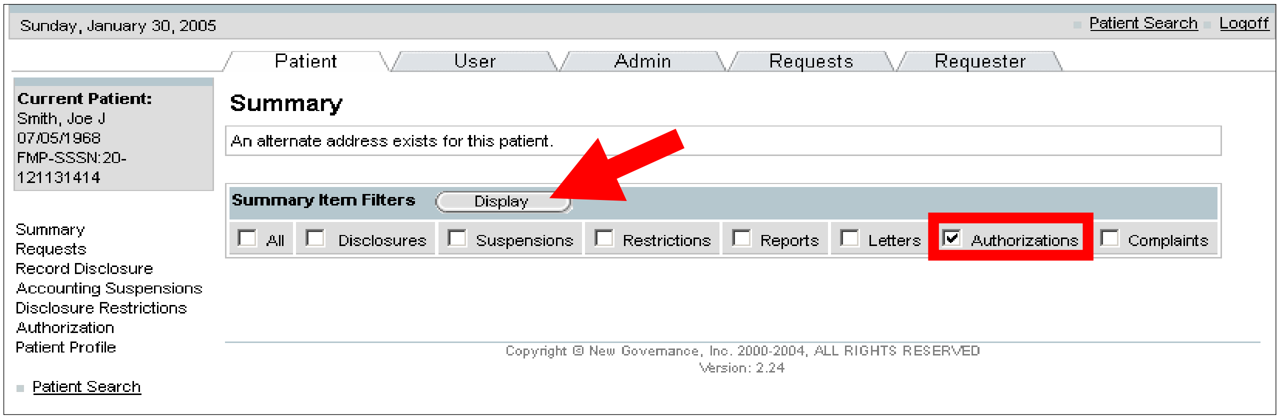
- A note appears at the top of the screen indicating the authorization is saved and that only the “Signed” or “Revoked” status fields may be changed at this point.

9. Select the Summary hyperlink.



10. Place a check in the Authorizations checkbox.

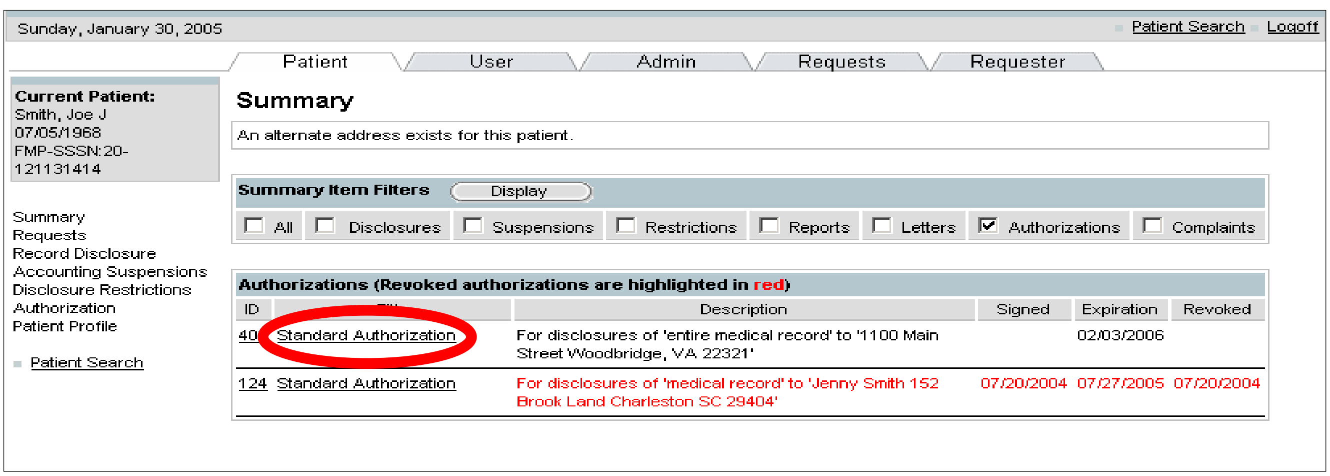
11. Click on the Display button.



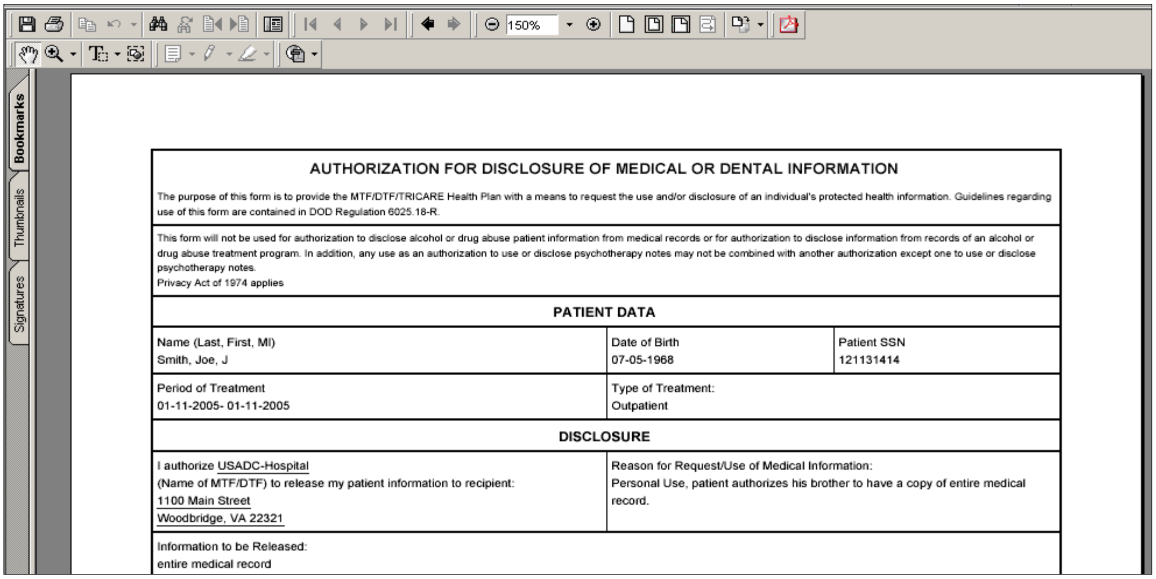
- The new authorization will appear on the Summary screen.

To generate the DD Form 2870 (Adobe Acrobat format):

1. Select the Authorization title hyperlink.



2. You may print the form and request the patient's signature.



AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION

The purpose of this form is to provide the MTF/DTF/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information. Guidelines regarding use of this form are contained in DOD Regulation 6025.18-R.

This form will not be used for authorization to disclose alcohol or drug abuse patient information from medical records or for authorization to disclose information from records of an alcohol or drug abuse treatment program. In addition, any use as an authorization to use or disclose psychotherapy notes may not be combined with another authorization except one to use or disclose psychotherapy notes.
Privacy Act of 1974 applies

PATIENT DATA

Name (Last, First, MI) Smith, Joe, J	Date of Birth 07-05-1968	Patient SSN 121131414
Period of Treatment 01-11-2005- 01-11-2005	Type of Treatment: Outpatient	

DISCLOSURE

I authorize USADC-Hospital (Name of MTF/DTF) to release my patient information to recipient: 1100 Main Street Woodbridge, VA 22321	Reason for Request/Use of Medical Information: Personal Use, patient authorizes his brother to have a copy of entire medical record.

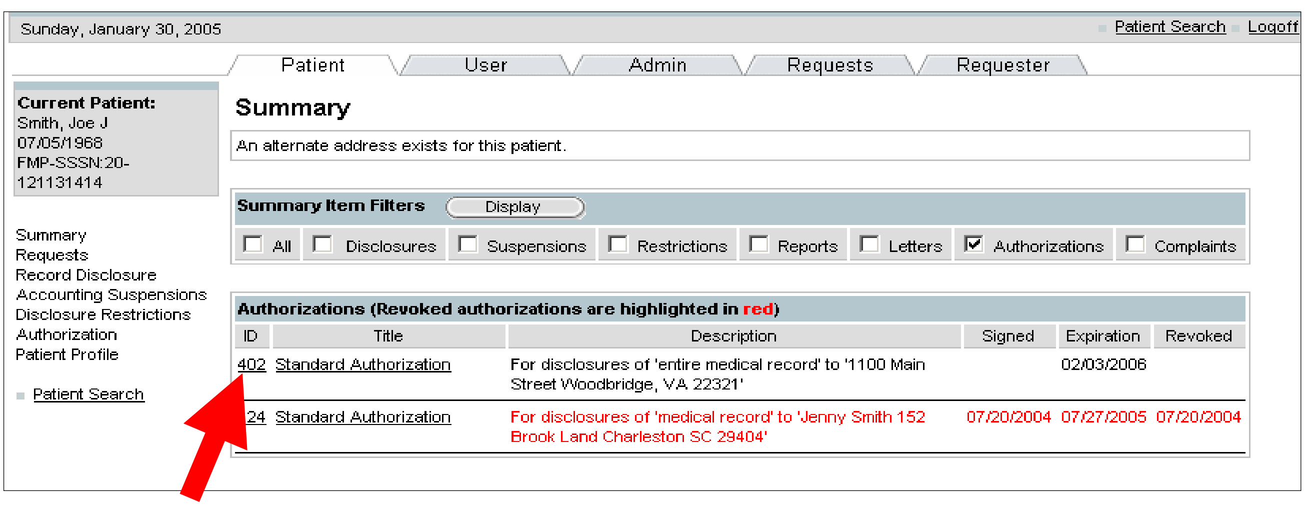
Information to be Released:
entire medical record

8.11 SIGN AN AUTHORIZATION

Once an authorization has been entered, it needs to be signed by the patient for validation. After the authorization is signed by the patient, a user has the ability to document the signature within the PHIMT.

To sign an authorization:

1. Select the authorization ID hyperlink to return to the detailed authorization record.

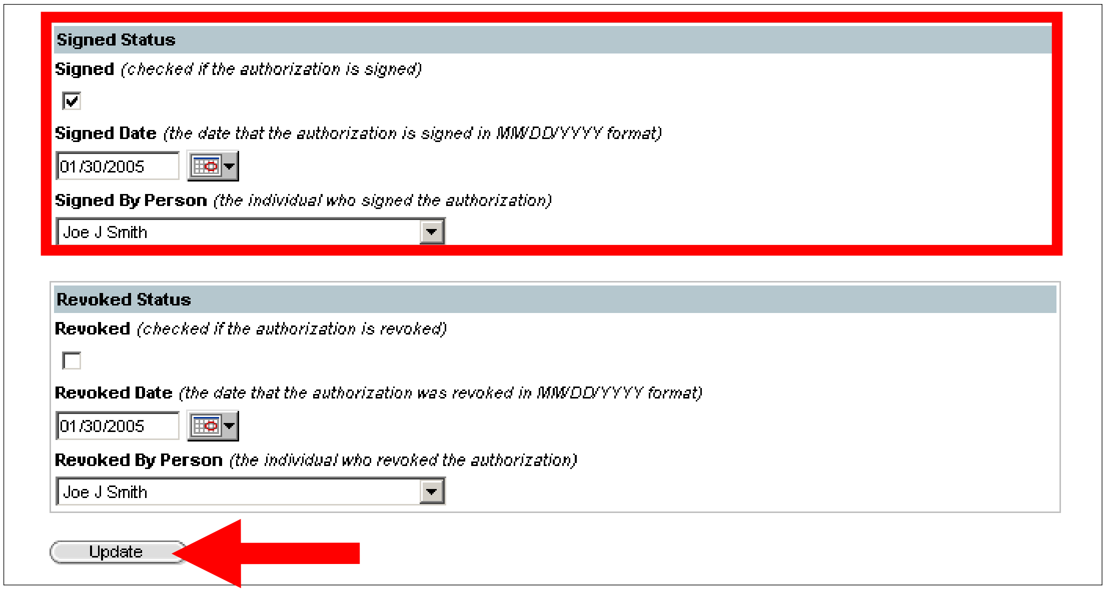


2. Scroll to the bottom of the page to the Signed Status box.

3. Place a check in the Signed Status checkbox.

4. Select the date and the authorizing person's identity from the drop-down box.

5. Click on the Update button.

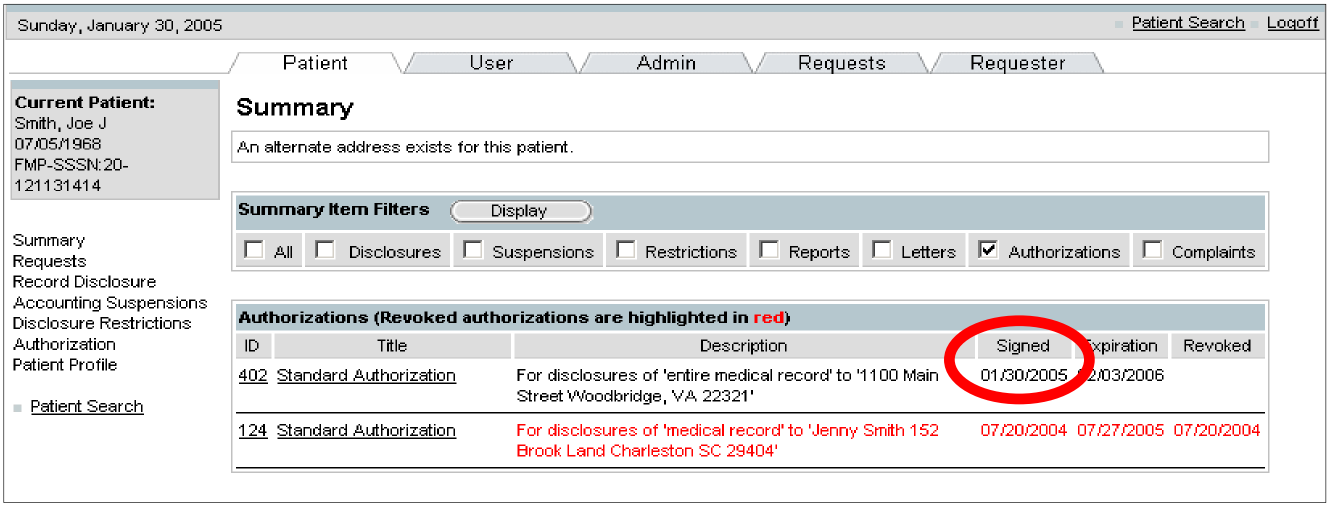


6. Select the Summary hyperlink.

7. Place a check in the Authorizations checkbox.

8. Click on the Display button.

- You will now see that the authorization indicates that it has been signed.



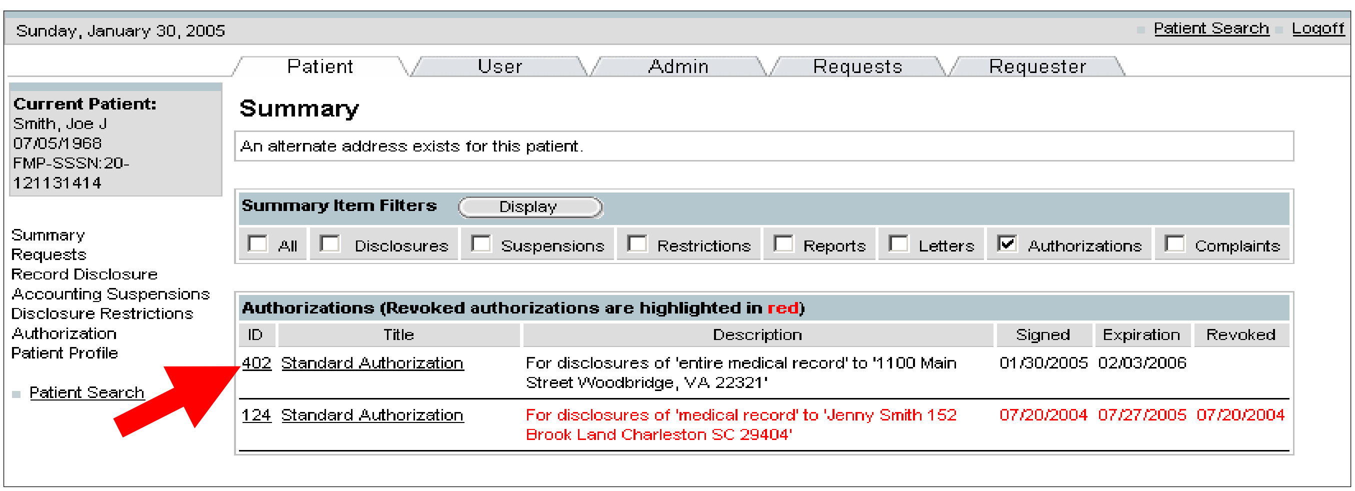
8.12 REVOKE AN AUTHORIZATION

Previously generated authorizations may need to be revoked as a result of legal issues, new information, or for other reasons.

To revoke an authorization:

1. Select the Patient Tab.

2. Select the Authorization ID hyperlink.

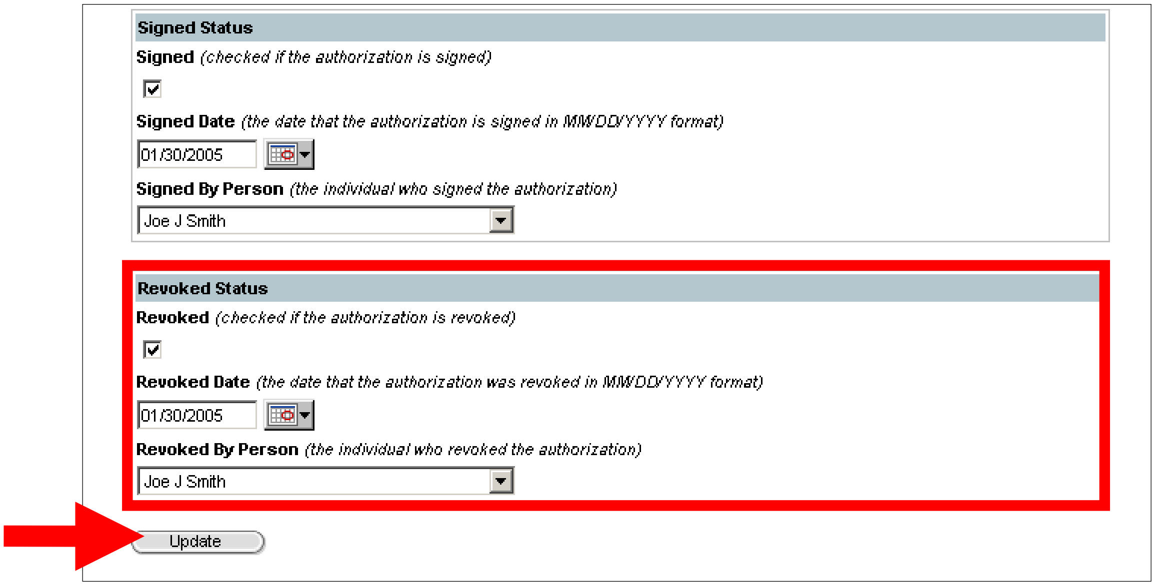


3. Scroll to the bottom of the screen to the Revoked Status box.

4. Place a check in the Revoked check box.

5. Select the date and the revoking person's identity in the drop-down box.

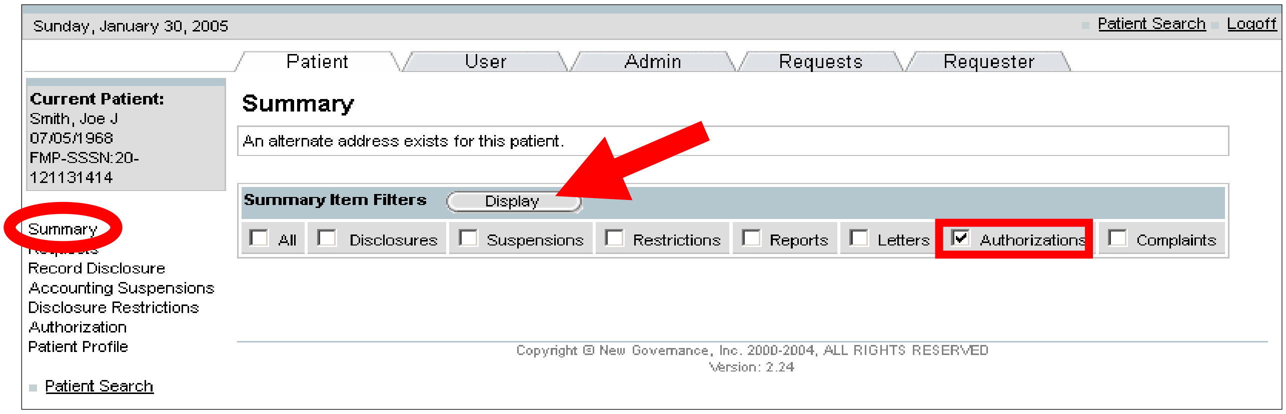
6. Click on the Update button.



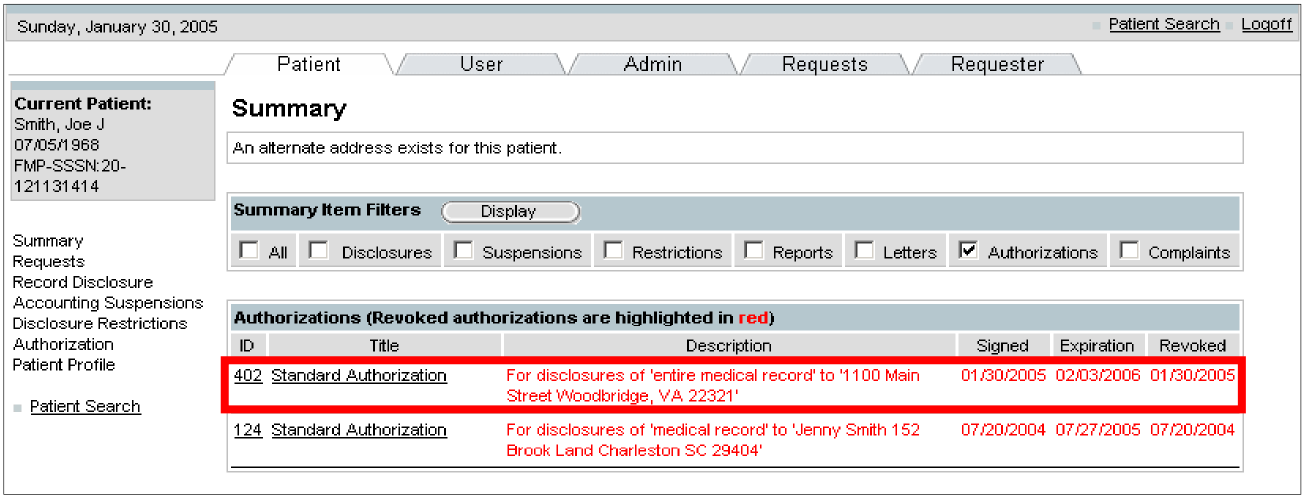
7. Select the Summary hyperlink to view the authorization.

8. Place a check in the Authorizations checkbox.

9. Click on the Display button.



- The revoked authorization is highlighted in red.



8.13 ADMINISTRATIVE SUMMARY REPORTS

Administrative summaries provide a visual representation by organization of:

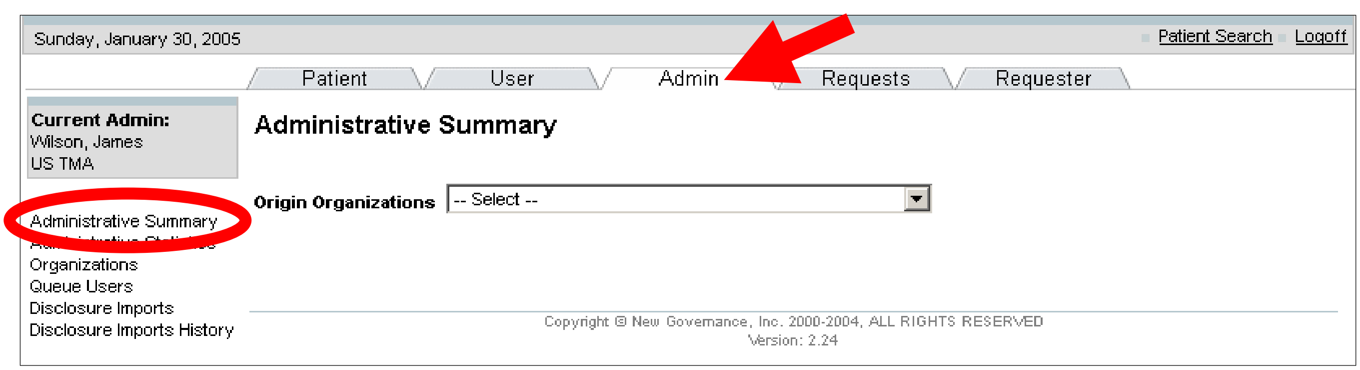
–Disclosures over a 12 month period
–All requests by type
–All requests over a 12 month period
–Top recipients of disclosures
–Top requesters for all requests

The Administrative Summary Reports are performed by Privacy Specialists and User Admins.

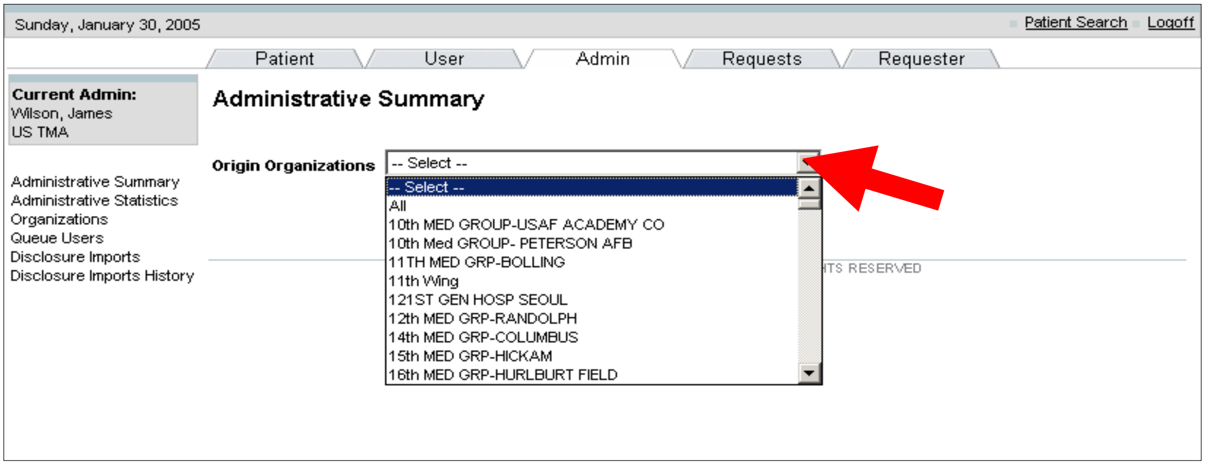
To create an Administrative Summary Report:

1. Select the Admin Tab.

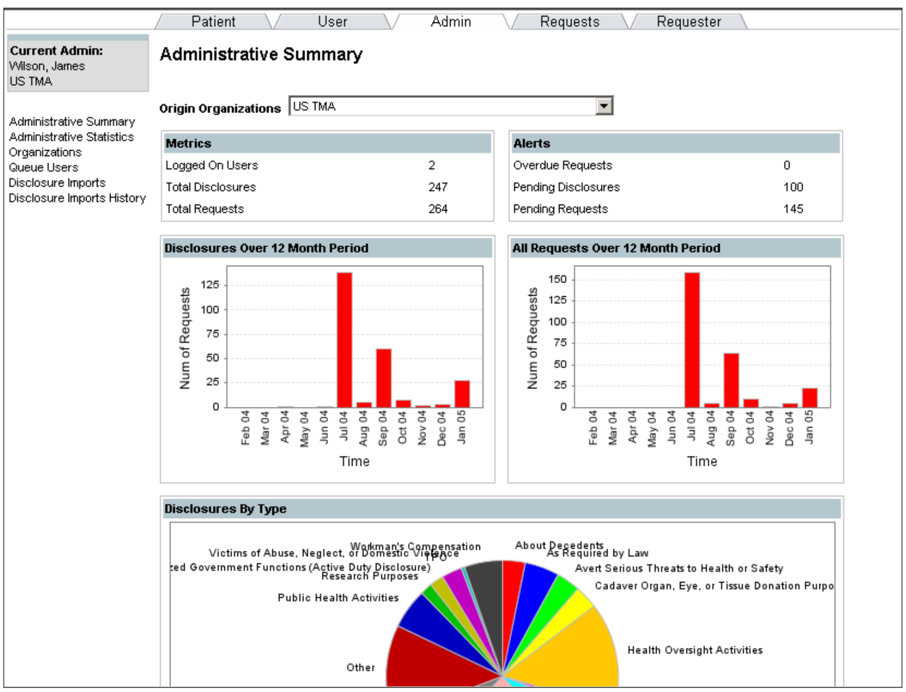
2. Select the Administrative Summary hyperlink.



3. Select your Organization from the drop-down box.



- The Administrative Summary reports will display.



9.0 PRIVACY SPECIALIST GLOSSARY

Accounting Suspension: In PHIMT, an accounting suspension is an action that results in the temporary postponement of a previously approved disclosure. The suspension can be either specific (referring to a particular disclosure) or type (referring to a disclosure of a particular type). Suspensions can be oral, lasting for up to thirty days, or written, lasting up to six months.

Admin Tab: The Admin tab is one of five label tags that provide access to user admin activities that include maintaining organizations in the PHIMT database.

Action: Action is a PHIMT term for a specific activity that requires a responsive judgment.

Attach: Attach is a PHIMT option that allows the user to send documentation or files with a disclosure.

Authorization: Authorization is a hyperlink on the Patient tab that allows the user to process an approval for a disclosure.

Back: Back is a navigation button that allows the user to return to the previous screen.

Complaint: Complaint is a PHIMT activity that allows a user to file a HIPAA grievance against a person or organization.

Create: Create is a PHIMT option that allows the user to initiate a new activity.

Create New Request: Create new request is a hyperlink on the Requests tab that allows the user to initiate a request for a new disclosure activity.

Disclosure: Disclosure is a hyperlink on the Requests tab that allows the user to process a release of protected health information.

Disclosure Accounting: Disclosure accounting is a hyperlink on the Requests tab that allows the user to process a justification for a disclosure.

Disclosure Details: Disclosure details is a PHIMT term that refers to information about a specific release that the user can view on the patient summary screen.

Disclosure Restriction: Disclosure restriction is a PHIMT term that refers to placing constraints on either the information being released or its recipient.

Display: Display is a PHIMT option that allows the user to view various types of information about a particular patient or disclosure activity.

Logoff: Logoff is a hyperlink that allows the user to exit PHIMT.

Login: Login is the PHIMT opening screen that requires a User ID and password.

MTF: MTF is a PHIMT acronym for Military Treatment Facility.

My Profile: My profile is a hyperlink on the User tab that allows a user to update personal information.

My Requests: My Requests is a hyperlink on the User tab that allows users to view the status of all requests initiated by them.

My Worklist: My Worklist is a hyperlink on the User tab that serves as an electronic inbox by allowing users to view all tasks currently assigned to them.

Next: Next is a PHIMT action button that allows the user to proceed to the next step in an activity.

New: New is a PHIMT action button that allows the user to develop a new item patient, organization.

New Patient Record: New patient record is a hyperlink on the Patient Search Results screen that allows users to provide information about a new patient.

Organization: In PHIMT, an organization is a logical or physical entity such as MTF, a service, or TMA.

Organization Management: Organization management is a hyperlink on the Admin tab that allows the privacy specialist to create and/or modify requester/recipient facilities within the PHIMT database. This term refers to the process of maintaining organization profiles and status.

Patient Profile: Patient Profile is a Hyperlink on the Patient tab that allows the user to create or edit patient information.

Patient Search: Patient Search is a hyperlink on the Patient tab that allows the user to look for a particular patient in the PHIMT database.

Patient Tab: Patient tab is a PHIMT tag or label that provides the user with patient specific activities.

PHI: PHI is an acronym for Protected Health Information.

PHIMT: PHIMT is an acronym for Protected Health Information Management Tool. PHIMT tracks disclosures of legally guarded-information with regards to HIPAA compliance.

Privacy Specialist: In PHIMT, A Privacy Specialist is the Privacy Officer or designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amend requests, and to restrict and suspend disclosures.

Record Disclosure: Record disclosure is a PHIMT term that refers to the documenting and confirmation of the release of protected health information.

Regular User: Regular user is a PHIMT general role with basic functionality. This role can create disclosures and authorization requests that can be routed to a Privacy Specialist.

Request: In PHIMT, a request is the first step in initiating a disclosure activity.

Request Action: In PHIMT, request action is a prompt for a specific performance on a disclosure.

Request Details: In PHIMT, request details allows the user to view relevant information about a particular disclosure.

Requester: In PHIMT, requester is a term that refers to the person making or issuing the activity.

Requester Profile: Requester profile is a hyperlink on the Requester tab that allows the user to view information about the individual or organization making the request.

Requester Requests: Requester requests is a hyperlink on the Requester tab that allows the user to view a listing of all requests made by a particular individual or organization.

Requester Search: Requester Search is a hyperlink on the Requester tab that allows the Privacy Specialist to look for the particular person or organization initiating the release of information.

Requester Summary: Requester summary is a hyperlink on the Requester tab that allows the user to view a brief of all requests initiated by an individual or organization.

Requester Tab: In PHIMT, the Requester tab is a tag or label that allows the user to access information about the individual or agency making a request for a disclosure.

Requests Tab: In PHIMT, the Requests tab is a tag or label that allows the user to access information about the activities requested by an individual or organization.

Restriction: In PHIMT, a restriction refers to a constraint put upon a particular disclosure activity. The constraint could refer to denying access to a particular individual or a particular time frame.

Revoke Authorization: In PHIMT, revoke authorization refers to a user rescinding a previous approval for a particular disclosure.

Routing: In PHIMT, routing refers to forwarding an approval for the disclosure request to your worklist for later action or to an individual of another role. For example, a Regular User may forward the approval request to a Privacy Specialist.

Save: Save is an action button that allows users to save data entries, information, and procedures.

Search: Search is an action button that allows users to search for a particular individual or activity.

Search for Request: Search for request is a hyperlink on the Requests tab that allows the user to look for a particular request made by that person.

Select: Select is an action button that allows users to select a particular patient or activity.

Status Box: In PHIMT, the status box is represented by a gray box in the upper left corner of all screens that displays the current information for a patient or activity; depending on actions being performed.

Summary: Summary is a hyperlink on the Patient tab that allows users to view a brief of all disclosure activities for a particular patient.

Summary Item Filter: Summary Item Filter is a feature accessed on the Patient Summary screen. This feature allows the user to display a synopsis on disclosures, suspensions, restrictions, reports, letters, and complaints.

Suspension: In PHIMT, Suspension refers to the act of delaying a disclosure or putting it on hold temporarily.

Switch Organizations: Switch Organizations is a hyperlink on the User tab that allows users who are assigned to more than one organization, to switch between their organizations. This allows them to change their primary status in an organization.

TMA: TMA is an acronym for Tricare Management Activity.

Update: Update is an action button that allows users to update information or perform additional activities.

User Profile: User Profile is a PHIMT term that is used when referring to the user preferences. This profile screen allows the regular user to update personal information and preference data about that user.

User Role: In PHIMT, role refers to a named collection of permissions. A role allows users with the same permissions to be grouped under a unique name such as: Regular User, User Admin, or Privacy Specialist. The MTF Privacy Officer usually determines the appropriate role.

User Search: User Search is a hyperlink on the Admin tab that allows the user admin to search for a particular user.

User Tab: The User tab is a tag or label that allows the user to access all PHIMT user related information. This tab is designed to track all tasks that are assigned to you.

User-to-User Relationship: User-to-User Relationship is a PHIMT term that refers to the different user types and how they work with one another. The User Admin creates this relationship as directed by the MTF Privacy Officer. The Privacy Officer understands how the MTF manages disclosures. The User Admin understands how to create a workflow by routing requests of a Regular User to a Privacy Specialist and from a Privacy Specialist to another Privacy Specialist, thereby creating the working relationships between the different PHIMT users. Multiple user relationships can be established throughout the Facility.

10.0 PRIVACY SPECIALIST ROLE PERMISSIONS

PHIMT PRIVACY SPECIALIST PERMISSIONS	
PHIMT Privacy Specialist Tab	**Enabled Permissions**
Logon/Logoff	Both
User Tab	Change password Switch to other organizations Update address User profile User workflow Workflow activity Workflow request Workflows tab
Admin Tab	Administrative workflow Attach file Backup person relationship Organization management
Patient Tab	Create patient New request: deny request now Patient accounting request Patient accounting suspensions Patient alternate communication Patient authorization Patient disclosure restrictions Patient profile Patient search Patient summary Patient workflow Record disclosure View disclosure
Requests Tab	Complaint workflow Disclosure accounting Disclosure request Disclosure imports Edit request: accept request Edit request: approve request Edit request: complete PHI retrieval Edit request: process complaint Edit request: route to another privacy specialist Edit request: route to other user New request: process request now New request: route to another privacy specialist New request: route to other user

PHIMT PRIVACY SPECIALIST PERMISSIONS	
PHIMT Privacy Specialist Tab	**Enabled Permissions**
	New request: route to My Worklist
Requester Tab	Requester summary Requester workflow